北京大学数学丛书

代　数　学

下　册

莫宗坚　蓝以中　赵春来　著

北 京 大 学 出 版 社

北京大学数学丛书

代 数 学

下 册

莫宗坚 等著

*

北京大学出版社出版

（北京大学校内）

北京大学印刷厂印刷

新华书店北京发行所发行 各地新华书店经售

850×1168毫米 32开本 9.5印张 236千字

1986年12月第一版 1986年12月第一次印刷

印数：1—12,000册

*

统一书号：13209·142 定价：2.30元

下 册 目 录

第六章 环 论

§1 环的局部化

本书所说的环都是有幺元的交换环．读者请参考第三章§2关于"比域"的讨论，特别是定义3.7中提出了"局部化环"的概念．在那里，我们假定了S是一整环，在本节中，我们将讨论一般环的情形．

定义6.1 设S为一环．S的一个非空子集D如果适合下列条件：

1） $0 \overline{\in} D$；

2） $d_1, d_2 \in D \Longrightarrow d_1 \cdot d_2 \in D$，

则称之为一**分母系**．

讨论 类似于定义3.7，我们想要定义s/d，这里$s \in S$，$d \in D$．自然的，就像从整数环$\boldsymbol{Z}$引出有理数域$\boldsymbol{Q}$的情形一样，我们要求

$$\frac{s_1}{d_1} + \frac{s_2}{d_2} = \frac{s_1 d_2 + s_2 d_1}{d_1 d_2}, \qquad \frac{s_1}{d_1} \cdot \frac{s_2}{d_2} = \frac{s_1 s_2}{d_1 d_2}.$$

麻烦的问题是$d \in D$可能是一个零因子，即有$s \in S$，$s \neq 0$，但$sd = 0$．则我们不免得出下面的自相矛盾的算式：

$$s = s \cdot 1 = s \cdot \left(d \cdot \frac{1}{d}\right) = (s \cdot d)\frac{1}{d} = 0 \cdot \frac{1}{d} = 0.$$

解决之道，是通过商环的步骤，消除这个难点．请见下定理．

定理6.1 令D为环S的一个分母系．又令

$$I = \{s: s \in S，存在一个 d \in D，使 sd = 0\}.$$

则有

1） I是S的一个理想；

2) 令 $\sigma: S \to S/I$ 为典型映射，则 $\sigma(D)$是S/I的一个分母系，而且，如果 $\sigma(s)\sigma(d)=0$，必有 $\sigma(s)=0$，此处 $d\in D$。

证明 1) 如果 $s_1, s_2 \in I$，则有 $d_1, d_2 \in D$，使

$$s_1 d_1 = 0, \quad s_2 d_2 = 0.$$

显然立得

$$(s_1 \pm s_2) d_1 d_2 = 0,$$

$$(s s_1) d_1 = s(s_1 d_1) = s \cdot 0 = 0, \quad \forall s \in S.$$

于是 I 是理想。

2) 显然，$\sigma(d_1)\sigma(d_2)=\sigma(d_1 d_2)\in\sigma(D)$。又如果 $0=\sigma(d)\in\sigma(D)$，立得 $d\in I$，即存在 $d_1\in D$，使 $0=dd_1\in D$。这与D的性质不合，所以 $0\bar{\in}\sigma(D)$。因此 $\sigma(D)$ 是一个分母系。

现设 $\sigma(s)\sigma(d)=0$，则 $\sigma(sd)=0$，即 $sd\in I$。故必存在$d_1\in D$，使 $s(dd_1)=(sd)d_1=0$。立得 $s\in I$，即 $\sigma(s)=0$。 ▎

讨论 从上面的定理，我们知道：给定一个分母系D以后，我们从环S转移到环S/I来考虑，则$\sigma(D)$中沒有零因子。因此，零因子所产生的难点也即消失。

定义6.2 设S是环，D是分母系。令I,σ如定理6.1所设。又令 $S'=S/I$，$D'=\sigma(D)$。则我们定义S对D的**局部化环** S_D为下面的集合

$$S_D = S'_{D'} = \left\{\frac{s'}{d'}: s'\in S',\ d'\in D'\right\},$$

及其运算规则

$$\frac{s'_1}{d'_1}+\frac{s'_2}{d'_2}=\frac{s'_1 d'_2 + s'_2 d'_1}{d'_1 d'_2},$$

$$\frac{s'_1}{d'_1}\cdot\frac{s'_2}{d'_2}=\frac{s'_1 s'_2}{d'_1 d'_2}, \qquad \frac{s'_1 d'_2}{d'_1 d'_2}=\frac{s'_1}{d'_1}.$$

又如果 $s'=\sigma(s)$，$d'=\sigma(d)$，则定义

$$\frac{s}{d}=\frac{s'}{d'}.$$

讨论 1）如果S为整环，则定义 6.2 与定义3.7相同。

2）对于分母系的规定，我们也可以取消$0 \overline{\in} D$的限制。自然，如果$0 \in D$时，$S_D = 0$。

例1 令$S = \boldsymbol{Z} \oplus \boldsymbol{Z}$，$D = \{(n, 0): n \neq 0\}$。则显然$D$是一个分母系。此时，不难看出

$$I = \{(0, m): m \in \boldsymbol{Z}\},$$

$$S/I \approx \boldsymbol{Z}, \quad \sigma(D) = \{n: n \neq 0\}.$$

于是，我们得出$S_D \approx \boldsymbol{Q}$。 ▌

我们任取$s \in S$，一般可以考虑

$$s \mapsto \sigma(s) \mapsto \frac{\sigma(s)\sigma(d)}{\sigma(d)}.$$

这样把S的元素s，认同为S_D的元素$\frac{\sigma(s)\sigma(d)}{\sigma(d)}$。例如，在例1中，把元素$(n, m)$认同为$n/1 = n$。显然，这个认同映射不是单射。

在下面的讨论中，我们将证明，环的局部化法与取商环法，是可以交换的。

定理6.2 设S是环，D是分母系，J是S的理想，$D \cap J = \varnothing$。令$\tau: S \to S_D$是认同映射。再令$J' = \tau(J) \cdot S_D$，即J'是J的元素在认同映射下的象所生成的理想。又令$\pi: S \to S/J$是典型映射。则恒有

$$\pi(S)_{\pi(D)} \approx S_D/J'.$$

证明 我们先要说明上面的式子是有意义的。换句话说，$\pi(D)$是$\pi(S)$的分母系。事实上，因为$D \cap J = \varnothing$，自然$0 \overline{\in} \pi(D)$。又有$\pi(d_1)\pi(d_2) = \pi(d_1 d_2) \in \pi(D)$ $(\forall d_1, d_2 \in D)$，所以$\pi(D)$是一个分母系。

我们定义一个映射α如下：

$$\alpha: \pi(S)_{\pi(D)} \to S_D/J',$$

$$\alpha\left(\frac{\pi(s)}{\pi(d)}\right) = \frac{s}{d} + J'.$$

请读者自行证明，这确实是个单满映射，故为同构。▌

我们常见的局部化环，是取$D=S\setminus\mathfrak{p}$，此处$\mathfrak{p}$是S的一个素理想。请注意，按照素理想的定义，我们有

$$ab\in\mathfrak{p}\implies a\in\mathfrak{p}\text{ 或 }b\in\mathfrak{p},$$

也即

$$a\overline{\in}\mathfrak{p},\ b\overline{\in}\mathfrak{p}\implies ab\overline{\in}\mathfrak{p},$$

$$a\in D,\ b\in D\implies ab\in D,$$

因此，$D=S\setminus\mathfrak{p}$确是一个分母系。

符号 设$D=S\setminus\mathfrak{p}$，$\mathfrak{p}$是素理想，则我们用$S_\mathfrak{p}$表示S_D。又设$J\subset S$，$\tau: S\to S_\mathfrak{p}$是认同映射，则我们用$JS_\mathfrak{p}$表示$\tau(J)S_\mathfrak{p}$，即由$\tau(J)$生成的理想。

例2 令$S=\mathbf{C}[x,y]$，$\mathfrak{p}=(x-a,y-b)$，则有

$$S_\mathfrak{p}=\left\{\frac{f(x,y)}{g(x,y)}: f,g\in S,\ g(a,b)\neq 0\right\}.$$

不难看出，$S_\mathfrak{p}$即是在点(a,b)有定义的有理函数的集合。

又令$R=\{(f(x),g(y)): f,g\in S,\ f(0)=g(0)\}$，即定义在$x$轴及$y$轴上的多项式组（任何一组中的两个多项式在原点取值相等）的集合。令$\mathfrak{q}=\{(xf(x),yg(y))\}$，则有

$$R_\mathfrak{q}=\left\{\left(\frac{f(x)}{r(x)},\frac{g(x)}{s(x)}\right): r(0)\neq 0,\ s(0)\neq 0,\ \frac{f(0)}{r(0)}=\frac{g(0)}{s(0)}\right\}.$$

不难看出，$R_\mathfrak{q}$即是在原点有定义的x轴及y轴上的有理函数组（每组中的两个有理函数在原点取值相等）的集合。

定义6.3 设环S中只有唯一的极大理想$\mathfrak{m}$，则称S为**局部环**。

讨论 定理3.23中已经证明，在任意环S中必有一极大理想。在局部环的定义中，我们强调只有唯一的极大理想。

定理6.3 1）环S是局部环$\iff J=\{s\in S: s\text{ 非可逆元}\}$是一个理想。于是$J$是$S$的唯一的极大理想；

2）设$\mathfrak{p}$是环S的素理想，则$\mathfrak{p}S_\mathfrak{p}$是$S_\mathfrak{p}$的唯一的极大理想。

于是$S_\mathfrak{p}$是局部环。

证明 1) $\Longrightarrow$. 令$\mathfrak{m}$是S的极大理想，则显然$\mathfrak{m}=J$.

$\Longleftarrow$. 任取理想$I\neq S$，显然有$I\subset J$. 于是J是S的唯一的极大理想。

2) 令$s/d\in S_\mathfrak{p}$，其中$d\notin\mathfrak{p}$. 显然

$$\frac{d}{s}\in S_\mathfrak{p} \iff s\notin\mathfrak{p}.$$

所以s/d为可逆元当且仅当$s\notin\mathfrak{p}$，也即s/d为非可逆元当且仅当$s\in\mathfrak{p}$. 于是，$\mathfrak{p}S_\mathfrak{p}$是$S_\mathfrak{p}$中的所有非可逆元的集合，它显然是$S_\mathfrak{p}$的一个理想. 由1)，即知2)成立. ▎

例3 一般言之，任取环S的一个分母系D，则S对D的局部化环S_D不一定是局部环. 最简单的例子，令$D=\{1\}$，则$S_D=S$，显然不一定是局部环.

现在我们取一个实例. 令$S=\mathbf{C}[x,y]$，$\mathfrak{p}=(y-x^2)$. 请注意$y-x^2=0$定义一条抛物线. 我们考虑$S_\mathfrak{p}$，不难看出

$$S_\mathfrak{p}=\left\{\frac{f(x,y)}{g(x,y)}: g(x,x^2)\neq 0\right\}.$$

此时，分母$g(x,y)$不在抛物线$y-x^2=0$上恒等于零. 然而，在抛物线的个别点上，$g(x,y)$可以是零. 例如，y即可以当作分母，而此多项式y在原点$(0,0)$等于零. 自然，$(0,0)$是抛物线上的一点. ▎

值得我们注意的是S的理想在局部化后的变动情形，即在S_D中生成的理想如何. 我们有下面的定理.

定理6.4 1) 设D是环S的分母系，J是S的理想. 则

$$JS_D=S_D \iff J\cap D\neq\varnothing;$$

2) 设$\mathfrak{p}$及J是S的素理想，$J\subset\mathfrak{p}$. 则下面的映射是由S中含于$\mathfrak{p}$的素理想集合到$S_\mathfrak{p}$的素理想集合的单满映射：

$$J\mapsto JS_\mathfrak{p}.$$

证明 1) $\Longrightarrow$。令 $\tau: S\to S_D$ 是认同映射。已知 $JS_D=S_D$，所以有

$$1=\sum\tau(a_i)\frac{\tau(s_i)}{\tau(d_i)}=\frac{\tau(a)}{\tau(d)},\qquad s_i\in S,\ a_i,a\in J,\ d_i,d\in D.$$

即
$$\tau(a)=\tau(d),\qquad a-d\in\ker(\tau).$$
于是存在$d'\in D$，使$(a-d)d'=0$。立得 $J\ni ad'=dd'\in D$。

$\Longleftarrow$。显然。

2) 任取 I 为$S_\mathfrak{p}$的素理想。令
$$J=\{a: a\in S,\ aS_\mathfrak{p}\subset I\}.$$
则J显然是S的一个理想，以及$JS_\mathfrak{p}\subset I$。又任取$a/d\in I$，则 $a\in J$，以及 $a/d=a(1/d)\in JS_\mathfrak{p}$。于是 $I=JS_\mathfrak{p}$。又设 $ab\in J$，则 $abS_\mathfrak{p}\subset I$。用$I$ 是素理想这个条件，立得 $aS_\mathfrak{p}\subset I$ 或 $bS_\mathfrak{p}\subset I$，即 $a\in J$ 或 $b\in J$。所以J是 S 的一个素理想。这样，我们证明了映射 $J\mapsto JS_\mathfrak{p}$是满射。

现在我们假设 $JS_\mathfrak{p}=J'S_\mathfrak{p}$，$J$ 与 J' 都是含于 $\mathfrak{p}$ 的素理想，求证 $J=J'$。任取 $a\in J$，则有 $a/1\in JS_\mathfrak{p}=J'S_\mathfrak{p}$。所以有

$$\frac{a}{1}=\sum_i a'_i\frac{s_i}{d_i}=\frac{a'}{d},\qquad a'_i,a'\in J',\ s_i\in S,\ d_i,d\overline{\in}\mathfrak{p}.$$

也即
$$ad-a'\in\ker(\tau).$$
于是，存在 $d'\overline{\in}\mathfrak{p}$，使$(ad-a')d'=0\in J'$。但 $J'\subset\mathfrak{p}$，所以$d'\overline{\in}J'$，而 J' 为素理想，立得
$$ad-a'\in J',\qquad ad\in J',\qquad a\in J'.$$
因此 $J\subset J'$。同法可证 $J'\subset J$。即得 $J=J'$。故映射 $J\mapsto JS_\mathfrak{p}$是单射。 ▎

例4 对一般分母系D而言，$J\mapsto JS_D$不一定是单射。例如，取 $S=\boldsymbol{Z}\oplus\boldsymbol{Z}$，$D=\{(2n,0): n\neq0\}$。则不难看出

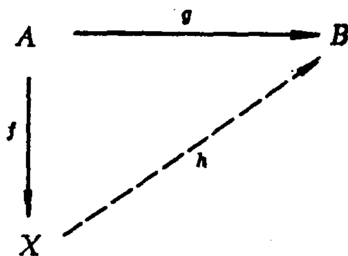
$$S_D=\left\{\frac{m}{2n}: m,n\in\boldsymbol{Z},\quad n\neq0\right\},$$

以及$(0)S_D=(\{0\}\oplus\mathbf{Z})S_D$，其中$(0)$表示$S$中的零理想。显然$\{0\}\oplus\mathbf{Z}$是$S$的一个非零理想。▎

任给一环S及两个非零因子a,b。则显然ab也为非零因子。所以，所有的非零因子的集合是一个分母系D。此时，S_D称为S的**全比环**。不难看出，当S是整环时，S的全比环即是S的比域。

习　题

1．证明局部化环可定义如下：设A是环，S是A的乘法封闭子集。一个环X称为A关于S的局部化环，如果存在一个环映射$f: A\to X$，使得对任一环映射$g: A\to B$，只要$g(s)$在B中可逆($\forall s\in S$)，必存在唯一的环映射$h: X\to B$，使得下面的图表交换：



2．设R是环，S是R的乘法封闭子集。如果对R的每个素理想$\mathfrak{p}$而言，

$$S\cap\mathfrak{p}\neq\varnothing,$$

问零是否一定在S中？

3．求$\mathbf{Z}/m\mathbf{Z}$的全比环，其中$m\in\mathbf{Z}$。

4．设R是主理想整环，证明局部化环R_D也是主理想整环。

5．设R是唯一分解环，证明R_D也是唯一分解环。

6．设R是一个局部环，I是R的真理想。证明R/I仍是局部环。

7. 证明$K[[x_1,x_2,\cdots,x_n]]$是一个局部环，这里K是一个域。

8. 证明在零点附近的复解析函数集$C\{\{x\}\}$是一个局部环。

9. 证明Z/p^nZ是一个局部环，其中p为素数，$n\in N$。

10. 令$R=Z/(60)$，$\mathfrak{p}=2R$。求$R_\mathfrak{p}$的基数。

11. 设R是整环。证明$R=\bigcap R_\mathfrak{m}$，此式右端的交集是对R的所有极大理想$\mathfrak{m}$而言的。

12. 设$Z\subset R\subset Q$，R是一个局部环。证明$R=Z_{(p)}$或Q，此处p是一个素数。

13. 设K是域，$K[x]\subset R\subset K(x)$，$R$是局部环。证明$R=K[x]_{(f(x))}$或$K(x)$，此处$f(x)$是$K[x]$中一个不可约多项式。

§2 整数扩充

我们考虑$Z\subset Q$。任意有理数$a\in Q$，都适合下面形式的整系数方程式

$$nx-m=0,\quad n,m\in Z,\ (n,m)=1.$$

而且

$$a\in Z\Longleftrightarrow n=1.$$

又，我们熟悉的$\sqrt{2}\notin Q$的一个古典证法如下：首先，$\sqrt{2}$适合下式：

$$x^2-2=0,$$

然后再应用下面的定理。

定理6.5 设a为有理数。如果a适合下面的整系数首一多项式

$$x^n+a_1x^{n-1}+\cdots+a_n=0,\quad a_i\in Z,$$

则a必为整数。

证明 令$a=m/d$为既约分数，即$(m,d)=1$。代入上式化简，则得

$$m^n = d(-a_1 m^{n-1} - \cdots - a_n d^{n-1}).$$

即有 $d|m^n$，所以 $d = \pm 1$。于是 $a = m/d \in \mathbf{Z}$。 ▎

从定理6.5，我们知道，如果$\sqrt{2}$是有理数，则必是整数。显然 $x^2 - 2 = 0$ 沒有整数根，因此$\sqrt{2}$必非有理数。

类似于上面对整数的刻划方法，我们给出下面的定义。

定义6.4 给定两环 $S \subset R$。设 $r \in R$，如果 r 适合下面的首一方程式 $f(x) \in S[x]$：

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_n = 0, \quad a_i \in S,$$

则称 r 对 S 为**整数相关的**。

与定理6.5完全一样，我们可以证明下面的定理。

定理6.5′ 设 S 是唯一分解整环，K 是 S 的比域。如果 $r \in K$ 对 S 为整数相关的，则 r 必在 S 中。

证明 读者自证之。 ▎

例5 取 $\mathbf{C}[x, 1/x] \supset \mathbf{C}[x]$。则$1/x$不是对 $\mathbf{C}[x]$整数相关的。我们可以把 $\mathbf{C}[x, 1/x]$表示成$\mathbf{C}[x, y]/(xy-1)$。从几何观点来看，$xy - 1 = 0$ 当 $x = 0$ 时无解，即双曲线 $xy - 1 = 0$ 上不存在任何一点，它向 x 轴的投影为原点。这恰是 $y = 1/x$对$\mathbf{C}[x]$非整数相关的几何意义。一般来说，如果 y 适合下面的方程式

$$a_0(x) y^n + a_1(x) y^{n-1} + \cdots + a_n(x) = 0,$$

而其中 $a_0(x)$不是常数，则 $a_0(x) = 0$ 所决定的 x 点上，y 的解数将少于 n。因此，y 所适合的方程式是否是首一的，有很大的几何意义。 ▎

我们要仿照域论中对代数相关的研究来处理环论中的整数相关。在域论中，我们应用向量空间的理论，在环论中，我们要采用模论了。

定理6.6 给定两环 $S \subset R$，$r \in R$，则下列条件是等同的：

1） r 对 S 是整数相关的；

2） $S[r]$是有限 S 模；

3） 存在一个有限 S 模 $M \subset R$，使 $1 \in M$，$rM \subset M$。

证明 1)$\Longrightarrow$2)。设 r 适合 $r^n+a_1r^{n-1}+\cdots+a_n=0$。则有

$$
\begin{aligned}
r^n &= -a_1r^{n-1}-\cdots-a_n,\\
r^{n+1} &= -a_1r^n-\cdots-a_nr\\
&= -a_1(-a_1r^{n-1}-\cdots-a_n)-a_2r^{n-1}-\cdots-a_nr\\
&= b_1r^{n-1}+\cdots+b_n, \qquad b_1,\cdots,b_n\in S,
\end{aligned}
$$

等等。不难看出，$r^n,r^{n+1},\cdots\in S\cdot 1+S\cdot r+\cdots+S\cdot r^{n-1}$，于是 $\{1,r,\cdots,r^{n-1}\}$是 $S[r]$的有限生成元集，即 $S[r]$是有限 S 模。

2)$\Longrightarrow$3)。令$M=S[r]$即可。

3)$\Longrightarrow$1)。设$\{m_1,\cdots,m_n\}$是M的有限生成元集。按照条件3)，我们得出

$$
\begin{aligned}
rm_1 &= a_{11}m_1+\cdots+a_{1n}m_n,\\
&\cdots\cdots\cdots\cdots\cdots\cdots \qquad a_{ij}\in S.\\
rm_n &= a_{n1}m_1+\cdots+a_{nn}m_n,
\end{aligned}
$$

应用初等线性代数的 Cramer 法则，立得

$$
\det\begin{bmatrix} r-a_{11} & -a_{12} & \cdots & -a_{1n}\\ -a_{21} & r-a_{22} & \cdots & -a_{2n}\\ \cdots & \cdots & \cdots & \cdots\\ -a_{n1} & -a_{n2} & \cdots & r-a_{nn}\end{bmatrix}\cdot m_i=0, \qquad i=1,\cdots,n.
$$

将上式左端的“特征行列式”展开成

$$f(r)=r^n+a_1r^{n-1}+\cdots+a_n \quad (a_i\in S),$$

则有

$$f(r)\cdot m=0, \qquad \forall m\in M.$$

取$m=1$，即有$f(r)=0$。所以 r 是对 S 整数相关的。▎

应用上面的定理，我们可以证明：

定理6.7 给定两环 $S\subset R$。则R中所有对S为整数相关的元素构成一环S'。此环S'具有如下性质：如果$r\in R$对S'为整数相关的，则必有$r\in S'$。S'称为S在R中的**整数闭包**。

证明 任取$r\in R$对S为整数相关的，再任取$g(r)\in S[r]$。

在上面的定理中，令$M=S[r]$，则显然有$1\in M$及$g(r)M\subset M$。所以$g(r)$对S是整数相关的。我们证明了$S[r]\subset S'$。

任取$r_1,r_2\in S'$。显然，r_2是对$S[r_1]$为整数相关的。于是

$$S[r_1,r_2]=S[r_1][r_2]$$

是有限$S[r_1]$模。而$S[r_1]$又是有限S模，不难得出$S[r_1,r_2]$是有限S模。任取$h(r_1,r_2)\in S[r_1,r_2]$，令$M=S[r_1,r_2]$，应用定理6.6，立得$h(r_1,r_2)$对S是整数相关的。所以$S[r_1,r_2]\subset S'$。因此，S'当然是一环。

我们又取$r\in R$对S'是整数相关的。设r适合下式：

$$r^n+s_1'r^{n-1}+\cdots+s_n'=0, \quad s_i'\in S',$$

则$S[s_1',\cdots,s_n',r]$是有限$S[s_1',\cdots,s_n']$模。不难看出，$S[s_1',\cdots,s_n']$是有限S模，于是，$S[s_1',\cdots,s_n',r]$是有限S模。因此，r是对S整数相关的，也即$r\in S'$。❙

为了眉目清晰起见，我们给出下面的定义。

定义6.5 设环S的全比环是R。如果S在R中的整数闭包就是S自身，则称S是整数封闭的。

讨论 参考定理6.5′，任意一唯一分解整环都是整数封闭的。例如，任取一域K，则多项式环$K[x_1,\cdots,x_n]$是整数封闭的。❙

我们有下面的重要定理。

定理6.8（诺德正规化定理） 设K是域，$R=K[r_1,\cdots,r_m]$是一个整环，此处$r_1,\cdots,r_m$不一定是变数。则必存在变数$x_1,\cdots,x_n\in R$，使得R的任意元素r都是对$S=K[x_1,\cdots,x_n]$整数相关的。

证明（永田雅宜证法） 取变数$y_1,\cdots,y_m$。定义下面的环映射

$$\sigma: K[y_1,\cdots,y_m]\to K[r_1,\cdots,r_m],$$
$$\sigma(y_i)=r_i, \quad i=1,\cdots,m.$$

如果$\ker(\sigma)=(0)$，则$K[y_1,\cdots,y_m]\approx K[r_1,\cdots,r_m]$，也即$r_1,\cdots,r_m$是变数。此时我们令$x_i=r_i$，$S=R$即可。以下，我们假

设 $\ker(\sigma)\neq(0)$。任取 $f(y_1,\cdots,y_m)\in\ker(\sigma)$，$f(y_1,\cdots,y_m)\neq 0$，读者不难看出(请补足之)，适当选取正整数

$$0\ll l_2\ll l_3\ll\cdots\ll l_m,$$

可以用下面的变数代换

$$z_1=y_1,$$
$$z_2=y_2-y_1^{l_2}=y_2-z_1^{l_2},$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$z_m=y_m-y_1^{l_m}=y_m-z_1^{l_m},$$

使得

$$f(z_1,z_2+z_1^{l_2},\cdots,z_m+z_1^{l_m})$$
$$=a_0z_1^l+a_1(z_2,\cdots,z_m)z_1^{l-1}+\cdots+a_l(z_2,\cdots,z_m),$$

其中 $a_0\in K$，$a_0\neq 0$。至此，再相应地令

$$r_1'=r_1,$$
$$r_2'=r_2-r_1^{l_2}=r_2-(r_1')^{l_2},$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$r_m'=r_m-r_1^{l_m}=r_m-(r_1')^{l_m},$$

不难看出，$K[r_1,\cdots,r_m]=K[r_1',\cdots,r_m']$，以及

$$a_0(r_1')^l+a_1(r_2',\cdots,r_m')(r_1')^{l-1}+\cdots+a_l(r_2',\cdots,r_m')=0.$$

所以 r_1' 对 $K[r_2',\cdots,r_m']$ 是整数相关的。于是，我们可以用 $K[r_2',\cdots,r_m']$ 代替上面的 $K[r_1,\cdots,r_m]$，然后再重新讨论。如此逐步作下去，即得本定理。▌

例6 考虑例5，$\boldsymbol{C}[x+(1/x)]\subset\boldsymbol{C}[x,1/x]$ 适合定理6.8的要求，即 $\boldsymbol{C}[x,1/x]$ 中任意元素都是对 $\boldsymbol{C}[x+(1/x)]$ 整数相关的。而 $\boldsymbol{C}[x]\subset\boldsymbol{C}[x,1/x]$ 与 $\boldsymbol{C}[1/x]\subset\boldsymbol{C}[x,1/x]$ 都不适合定理6.8的要求。从几何观点看来，就是说，从双曲线 $xy-1=0$ 向 x 轴或 y 轴投影，都不适当。如果向直线 $x+y=0$ 投影，则有某种正则性(即对于直线 $x+y=0$ 上任一点 P，都有双曲线 $xy-1=0$ 上的两个点投影到 P 上)。其代数观点上的含意，请见下定理。

定理6.9(Cohen 及 Seidenberg 上升定理) 设有两环 $S\subset R$，

而且R的元素都对S整数相关。那么，任取素理想$\mathfrak{p}\subset S$，必有素理想$\mathfrak{q}\subset R$，使$\mathfrak{q}\cap S=\mathfrak{p}$。

证明 我们先处理S是局部环，$\mathfrak{p}$是它的唯一极大理想的情形。此时，任取R的一个极大理想$\mathfrak{q}$，自然，$\mathfrak{q}$是素理想。令$\mathfrak{p}'=\mathfrak{q}\cap S$。我们有下图：

$$\begin{array}{ccc} R & \longrightarrow & R/\mathfrak{q} \\ \cup & & \cup \\ S & \longrightarrow & S/\mathfrak{p}' \end{array}$$

显然，域$R/\mathfrak{q}$的元素对$S/\mathfrak{p}$都是整数相关的。下面的引理将证明$S/\mathfrak{p}'$也是域。因此$\mathfrak{p}'$是一个极大理想，即有$\mathfrak{p}'=\mathfrak{p}$。

在一般情形下，令$D=S\backslash\mathfrak{p}$。考虑$S_D$及$R_D$。此时，任取$r/d\in R_D$，设$r$适合下式：

$$r^n+a_1r^{n-1}+\cdots+a_n=0\,,\qquad a_i\in S,$$

则有

$$\left(\frac{r}{d}\right)^n+\frac{a_1}{d}\left(\frac{r}{d}\right)^{n-1}+\cdots+\frac{a^n}{d^n}=0\,,$$

即r/d对S_D为整数相关的。请注意$R_D\supset S_D$，而且S_D是局部环，$\mathfrak{p}S_D$是它的唯一极大理想。因此，应用上半部的证明，我们有R_D的素理想$\mathfrak{q}'R_D$，使$\mathfrak{q}'R_D\cap S_D=\mathfrak{p}S_D$。参考下图

$$\begin{array}{ccc} R & \stackrel{\tau}{\dashrightarrow} & R_D \\ \cup & & \cup \\ S & \stackrel{\tau}{\longrightarrow} & S_D \end{array}$$

令$\mathfrak{q}=\tau^{-1}(\mathfrak{q}'R_D)$，则有

$$\begin{aligned}\mathfrak{q}\cap S&=\tau^{-1}(\mathfrak{q}'R_D)\cap S=\tau^{-1}(\mathfrak{q}'R_D\cap S_D)\\&=\tau^{-1}(\mathfrak{p}S_D)=\mathfrak{p}. \quad \blacksquare\end{aligned}$$

引理 设$S\subset R$是二整环，R的元素对S都是整数相关的。则S是域$\Longleftrightarrow R$是域。

证明 $\Longrightarrow$。域论。

$\Longleftarrow$. 任取 $a\in S$, $a\neq 0$。则 $a\in R$, $1/a\in R$。令 $1/a$ 适合下式:

$$\left(\frac{1}{a}\right)^n + b_1\left(\frac{1}{a}\right)^{n-1} + \cdots + b_n = 0, \qquad b_i\in S.$$

乘以 a^{n-1}, 立得

$$\frac{1}{a} = -b_1 - b_2 a - \cdots - b_n a^{n-1} \in S.$$

即 S 的任意非零元素都是可逆的。因此 S 是域。 ▎

讨论 1) 这个引理也是定理6.9的特例: 任取 S 的一个极大理想 $\mathfrak{p}$, 则必有 R 的一个素理想 $\mathfrak{q}$, 使 $\mathfrak{p}=\mathfrak{q}\cap S$。如果 R 是域, 则它的唯一的素理想 $\mathfrak{q}=(0)$。因此 $\mathfrak{p}=(0)\cap S=(0)$。从这点我们易于推知 S 是域。

2) 回过头来, 我们再看定理6.8. 在 n 维空间中任取一点 $(a_1,\cdots,a_n)$, 它对应于素理想

$$(x_1-a_1, x_2-a_2, \cdots, x_n-a_n)\subset S=K[x_1,\cdots,x_n].$$

于是必存在一素理想 $\mathfrak{q}\subset R$, 使 $\mathfrak{q}\cap S=(x_1-a_1,\cdots,x_n-a_n)$。用几何的术语来说, $\mathfrak{q}\cap S$ 即是向 n 维空间的投影。但是 $\mathfrak{q}$ 相应于什么呢? 在下一节中, 我们将说明, $\mathfrak{q}$ 相应于几何学中的点。综上所述, 定理6.8是说: 给定了一个相应于 R 的"代数多样体" V, 我们可以找到一个 n 维空间 A^n, 使从 V 到 A^n 的投影是满射. 进而言之,它不仅是满射,还有其它的优良性质。详情见后。

3) 在定理6.9的条件下, 如果有两个素理想 $\mathfrak{p}_1\subset\mathfrak{p}_2\subset S$, 及素理想 $\mathfrak{q}_1\subset R$, 使 $\mathfrak{q}_1\cap S=\mathfrak{p}_1$, 自然 $S/\mathfrak{p}_1\subset R/\mathfrak{q}_1$ 同样适合定理6.9的条件。于是, 存在 $\mathfrak{q}_2(R/\mathfrak{q}_1)\cap S/\mathfrak{p}_1=\mathfrak{p}_2(S/\mathfrak{p}_1)$。不难看出, 素理 $\mathfrak{q}_2$ 适合 $\mathfrak{q}_1\subset\mathfrak{q}_2$ 及 $\mathfrak{q}_2\cap S=\mathfrak{p}_2$. 这可用下式表示:

$$\begin{matrix} R\supset\mathfrak{q}_2\supset\mathfrak{q}_1, \\ \cup \\ S\supset\mathfrak{p}_2\supset\mathfrak{p}_1, \end{matrix} \qquad \mathfrak{q}_1\cap S=\mathfrak{p}_1,\ \mathfrak{q}_2\cap S=\mathfrak{p}_2.$$

我们很容易把上面的讨论推广到 S 的一个素理想链 $\mathfrak{p}_n\supset\mathfrak{p}_{n-1}$

$\supset\cdots\supset\mathfrak{p}_1$及$R$的素理想$\mathfrak{q}_1(\mathfrak{q}_1\cap S=\mathfrak{p}_1)$的情形。根据定理6.9，必存在素理想$\mathfrak{q}_i$（$i=1,\cdots,n$），适合下式

$$\begin{array}{l} R\supset\mathfrak{q}_n\supset\cdots\supset\mathfrak{q}_1, \\ \cup \qquad\qquad\qquad\qquad \mathfrak{q}_i\cap S=\mathfrak{p}_i. \\ S\supset\mathfrak{p}_n\supset\cdots\supset\mathfrak{p}_1, \end{array}$$

我们将在环的"维数论"中，详细说明这个现象。

习　题

1. 证明定理6.5′。

2. 设S为整环，R是S在它的比域K中的整数闭包。令

$$C=\{a:\ a\in S,\ aR\subset S\}.$$

称C为S的**导子理想**(conductor)。证明C是S的理想，也是R的理想，并且C是同时为S及R的理想中的最大者。

3. 求$\boldsymbol{Z}$在p-adic域$\boldsymbol{Q}_p$中的整数闭包。

4. 令$R=\boldsymbol{C}[x,y]/(x^2-y^3)=\boldsymbol{C}[\bar{x},\bar{y}]$。求$R$在其比域中的整数闭包。

5. 令$R=\boldsymbol{C}[x,y]/(x^2-y^2-y^3)=\boldsymbol{C}[\bar{x},\bar{y}]$。求$R$在其比域中的整数闭包。

6. $\boldsymbol{Z}[x]/(x^2+3)$是否整数封闭？$\boldsymbol{Z}[x]/(x^2+5)$呢？

7. 设有环$A\subset B$。如果$B\backslash A$是B的乘法封闭子集，证明A在B中整数封闭。

8. 设整环R是整数封闭的，证明它的局部化环R_D也是整数封闭的。

9. 设整环R是整数封闭的，证明$R[x]$也是整数封闭的。

10. 设A是整数封闭的整环，K是A的比域，L/K是有限伽罗瓦扩张。设B是A在L中的整数闭包，证明

(1) $\sigma(B)=B,\ \forall\sigma\in G(L/K)$；

(2) $A=\{b:\ b\in B,\ \sigma(b)=b,\ \forall\sigma\in G(L/K)\}$。

11. 设有两个环$R\subset T$，如果对于T的每个素理想$\mathfrak{p}$，恒有

$T/\mathfrak{p}$对$R/R\cap\mathfrak{p}$是整数相关的，证明T对R是整数相关的。

12. 令$R=\boldsymbol{C}[x,y,z]/(z^2-xy)=\boldsymbol{C}[x,y,z]\supset\boldsymbol{C}[x,y]=S$，验证

$$(x,y)\supset(x+y^2)\supset(0)$$

是S的素理想链。试把这个链上升成R的素理想链。

13. 令$R=\boldsymbol{C}[x,y]/(xy-1)$。求$\boldsymbol{C}[z]\subset R$，使得$R$对$\boldsymbol{C}[z]$是整数相关的。参考定理6.8及例6，考虑其几何意义。

§3 零点定理

代数学的一个大问题是解多项式。在第五章的域论中，我们花了很多时间，考虑一个一元多项式的解，由此得出许多代数扩域的性质。推广来说，我们要求解下面的可能是无限多个方程联立的方程组：

$$f_i(x_1,\cdots,x_n)=0, \quad i=1,2,\cdots,$$

其中f_i都是多项式。我们先要确定它们有没有公解。令$I=(f_1(x_1,\cdots,x_n),f_2(x_1,\cdots,x_n),\cdots)$为它们生成的理想。则显然有

$$g(a_1,\cdots,a_n)=0, \quad \forall g(x_1,\cdots,x_n)\in I$$
$$\Longleftrightarrow f_i(a_1,\cdots,a_n)=0, \quad \forall i.$$

于是，求一组多项式的公解的问题，可化为求一个理想中的所有多项式的公解的问题。

现在我们给定一个理想$I\subset K[x_1,\cdots,x_n]$，此处$K$是一个域。如果$1\in I$，则下面的方程

$$1=0$$

无解。我们有下面的定理。

定理6.10（希尔伯特零点定理的弱式） 设K是一个代数封闭域，I是多项式环$K[x_1,\cdots,x_n]$的一个理想。则有

1） I是极大理想$\Longleftrightarrow I=(x_1-a_1,x_2-a_2,\cdots,x_n-a_n)$，其

中 $a_i \in K$ $(i=1,2,\cdots,n)$；

2) $1\in I \Longleftrightarrow I$无公解。

证明 1) $\Longleftarrow$。取下面的映射 σ：

$$\sigma: K[x_1,\cdots,x_n]\to K,$$
$$\sigma(f(x_1,\cdots,x_n))=f(a_1,\cdots,a_n).$$

显然，σ 是满射，及 $\ker(\sigma)=(x_1-a_1,\cdots,x_n-a_n)$。而$K$是域，故$(x_1-a_1,\cdots,x_n-a_n)$是极大理想。

$\Longrightarrow$。令 $K[\bar{x}_1,\cdots,\bar{x}_n]=K[x_1,\cdots,x_n]/I$，则$K[\bar{x}_1,\cdots,\bar{x}_n]$是域。应用诺德正规化定理，存在变数 $y_1,\cdots,y_m$，使

$$K[\bar{x}_1,\cdots,\bar{x}_n]\supset K[y_1,\cdots,y_m],$$

且 $K[\bar{x}_1,\cdots,\bar{x}_n]$的元素对 $K[y_1,\cdots,y_m]$都是整数相关的。应用上一节的引理，已知 $K[\bar{x}_1,\cdots,\bar{x}_n]$是域，所以 $K[y_1,\cdots,y_m]$也必然是域。然而 $K[y_1,\cdots,y_m]$又是多元多项式整环，通常不是域，除非没有任何变数存在。故

$$K[y_1,\cdots,y_m]=K.$$

于是 $K[\bar{x}_1,\cdots,\bar{x}_n]$是$K$的整数扩充，因此必是代数扩充。又已知$K$是代数封闭域，立得

$$K[\bar{x}_1,\cdots,\bar{x}_n]=K.$$

令

$$a_i=\bar{x}_i\in K\quad(i=1,\cdots,n),$$

则有 $x_i-a_i\in I$，即 $(x_1-a_1,\cdots,x_n-a_n)\subset I$。又前面已证出$(x_1-a_1,\cdots,x_n-a_n)$是极大理想，故有 $(x_1-a_1,\cdots,x_n-a_n)=I$。

2) $\Longrightarrow$。显然。

$\Longleftarrow$。设$1\bar{\in} I$，取一极大理想 $M\supset I$。根据 1)，

$$M=(x_1-a_1,\cdots,x_n-a_n)\supset I.$$

令 σ 为下面的映射：

$$\sigma: K[x_1,\cdots,x_n]\to K,$$
$$\sigma(f(x_1,\cdots,x_n))=f(a_1,\cdots,a_n).$$

则 $\ker(\sigma)=M\supset I$，即

$$\sigma(f(x_1,\cdots,x_n))=f(a_1,\cdots,a_n)=0, \qquad \forall f\in I.$$

于是，$(a_1,\cdots,a_n)$即是 I 的一个公解。 ▌

讨论 1) 希尔伯特零点定理建立了代数与几何的联系：一方面，我们有代数学中的极大理想，另一方面，我们有几何学中的点$(a_1,\cdots,a_n)$。这个定理告诉我们，下面的对应

$$(x_1-a_1,\cdots,x_n-a_n)\mapsto(a_1,\cdots,a_n),$$

当域K是代数封闭域时，是从多项式环 $K[x_1,\cdots,x_n]$的极大理想的集合到 A^n 中的点的集合的一个单满映射。

2) "K是代数封闭域"的条件显然是必要的。例如，我们取$K=\boldsymbol{R}$，则(x^2+1)是 $\boldsymbol{R}[x]$的一个极大理想，可是并不形如$(x-a)$。

3) 1是否属于I，这并不是一个一目了然的问题。可能要牵涉到繁复的计算才能决定。 ▌

在解多项式方程组 $f_i(x_1,\cdots,x_n)=0\ (i=1,2,\cdots)$ 时，或求一个理想 $I\subset K[x_1,\cdots,x_n]$的公解时，我们常碰到另一个问题。例如，令 $I=(x_1^2)$，则显然，$a_1^2=0\Longleftrightarrow a_1=0$。换句话说，$(x_1^2)$与$(x)$的公解是相同的。为了进一步去繁入简，我们引入下面的定义。

定义6.6 设 I 是环S的一个理想。我们定义 I 的**根理想**为

$$\sqrt{I}=\{a: a\in S,\ 存在某个正整数\ n,\ 使\ a^n\in I\}.$$

讨论 1) 易见$\sqrt{I}$是一个包含 I 的理想。而且我们有

(a) $\sqrt{I\cdot J}=\sqrt{I\cap J}=\sqrt{I}\cap\sqrt{J}$;

(b) $\sqrt{\sqrt{I}}=\sqrt{I}$;

(c) $\sqrt{I+J}=\sqrt{\sqrt{I}+\sqrt{J}}$.

事实上，设 $a,b\in\sqrt{I}$，则存在正整数 n,m，使 $a^n\in I$，$b^m\in I$。于是

$$(a+b)^{n+m}=\sum_{i=0}^{m+n}\binom{m+n}{i}a^ib^{m+n-i}.$$

显然，在上式中，或者 $l\geqslant n$，或者 $m+n-l\geqslant m$。于是易见

$$(a+b)^{m+n}\in I,$$

即 $a+b\in\sqrt{I}$。由此，读者不难论证 $\sqrt{I}$ 是包含 I 的一个理想：下面我们证明上面给出的三个公式。

(a) 一般言之，我们恒有(读者自证之)

$$I\cdot J\subset I\cap J\subset I.$$

不难得出，$\sqrt{I\cdot J}\subset\sqrt{I\cap J}\subset\sqrt{I}\cap\sqrt{J}$。现在，我们任取 $a\in\sqrt{I}\cap\sqrt{J}$，则 $a^n\in I$，$a^m\in J$，所以 $a^{nm}\in I\cdot J$，故 $a\in\sqrt{I\cdot J}$。这就是说 $\sqrt{I}\cap\sqrt{J}\subset\sqrt{I\cdot J}$。所以(a)中的三者都相等。

(b) 显然。

(c) 显然有 $I+J\subset\sqrt{I}+\sqrt{J}$，所以立得

$$\sqrt{I+J}\subset\sqrt{\sqrt{I}+\sqrt{J}}.$$

又有 $\sqrt{I+J}\supset\sqrt{I}$，$\sqrt{I+J}\supset\sqrt{J}$，我们导出

$$\sqrt{I+J}=\sqrt{\sqrt{I+J}}\supset\sqrt{\sqrt{I}+\sqrt{J}}.$$

2) 设 $I\subset K[x_1,\cdots,x_n]$，则 I 的公解与 $\sqrt{I}$ 的公解是相同的。 ▌

为了进一步建立代数与几何的联系，我们引入下面的定义。

定义6.7 1) 设 I 是 $K[x_1,\cdots,x_n]$ 中的一个理想。定义 I 的代数多样体(即 I 的公解) $\mathscr{V}(I)$ 为 n 维仿射空间 K^n 的一个子集：

$$\mathscr{V}(I)=\{(a_1,\cdots,a_n):(x-a_1,\cdots,x-a_n)\supset I\};$$

2) 设 $B\subset K^n$。定义 B 的理想 $\mathscr{I}(B)$ 为

$$\mathscr{I}(B)=\{f(x_1,\cdots,x_n):f(b_1,\cdots,b_n)=0,\ \forall(b_1,\cdots,b_n)\in B\}.$$

定理6.11(希尔伯特零点定理的强式) 设 K 是代数封闭域，$I\subset K[x_1,\cdots,x_n]$。则有

1) $\mathscr{I}(\mathscr{V}(I))=\sqrt{I}$；

2) $\mathscr{V}:I\to\mathscr{V}(I)$ 是从 $\{I:I=\sqrt{I}\}$ 到代数多样体集合的单满映射；

3) $\mathscr{I}: B \to \mathscr{I}(B)$ 是从代数多样体集合到 $\{I: I=\sqrt{I}\}$ 的单满映射。

证明 1) 显然有

$$f \in \sqrt{I} \Longrightarrow f^m \in I \Longrightarrow f^m \text{ 在 } \mathscr{V}(I) \text{ 上恒为零}$$
$$\Longrightarrow f \text{ 在 } \mathscr{V}(I) \text{ 上恒为零}$$
$$\Longrightarrow f \in \mathscr{I}(\mathscr{V}(I)),$$

这就是说，$\sqrt{I} \subset \mathscr{I}(\mathscr{V}(I))$。反过来，我们任取 $g \in \mathscr{I}(\mathscr{V}(I))$。令

$$J = I \cdot K[x_1, \cdots, x_n, x_{n+1}] + (1 - gx_{n+1}).$$

此时有两种可能性：$1 \overline{\in} J$ 或 $1 \in J$。

在第一种情形下，应用定理6.10(希尔伯特零点定理的弱式)，存在 $(x_1 - a_1, \cdots, x_n - a_n, x_{n+1} - a_{n+1}) \supset J$。自 然，$(a_1, \cdots, a_n) \in \mathscr{V}(I)$。于是我们得到下面两个互相矛盾的式子：

$$1 - g(a_1, \cdots, a_n)a_{n+1} = 0, \qquad g(a_1, \cdots, a_n) = 0.$$

所以，不可能有 $1 \overline{\in} J$。

现在，我们知道 $1 \in J$。于是有

$$f_i(x_1, \cdots, x_n) \in I \qquad (i = 1, 2, \cdots, l),$$

使下式成立

$$1 = \sum_{i=1}^{l} h_i(x_1, \cdots, x_{n+1}) f_i(x_1, \cdots, x_n)$$
$$+ (1 - g(x_1, \cdots, x_n)x_{n+1}) h_{l+1}(x_1, \cdots, x_{n+1}),$$

其中 $h_i(i = 1, \cdots, l, l+1)$ 均为 $K[x_1, \cdots, x_n, x_{n+1}]$ 中的多项式。既然上式是恒等式，我们可以令 $x_{n+1} = g^{-1}$。代入后，有

$$1 = \sum_{i=1}^{l} h_i(x_1, \cdots, x_n, 1/g) f_i(x_1, \cdots, x_n).$$

两边乘以 g 的适当的方幂 g^s，得

$$g^s = \sum_i g_i(x_1, \cdots, x_n) f_i(x_1, \cdots, x_n) \in I,$$

也即 $g\in\sqrt{I}$，所以 $\mathscr{I}(\mathscr{V}(I))\subset\sqrt{I}$。

2)及 3) $\mathscr{I}(\mathscr{V}(I))=\sqrt{I}=I$，$\mathscr{V}(\mathscr{I}(\mathscr{V}(I)))=\mathscr{V}(\sqrt{I})$ $=\mathscr{V}(I)$。所以 $\mathscr{I}\cdot\mathscr{V}$ 是恒等映射，$\mathscr{V}\cdot\mathscr{I}$ 是恒等映射。因此 $\mathscr{I}$，$\mathscr{V}$ 都是单满映射。▌

讨论 上面的定理，建立了代数与几何的关系。进一步说，我们有下面的定理。

定理6.12 设 I,J,I_i 是 $K[x_1,\cdots,x_n]$ 的理想，K 是代数封闭域，B_i 是仿射空间 K^n 的子集。我们恒有

1) $I\subset J\Longrightarrow\mathscr{V}(I)\supset\mathscr{V}(J)$；

2) $B_1\subset B_2\Longrightarrow\mathscr{I}(B_1)\supset\mathscr{I}(B_2)$；

3) $\mathscr{V}\left(\sum_i I_i\right)=\bigcap\mathscr{V}(I_i)$；

4) $\mathscr{V}(I\cap J)=\mathscr{V}(I)\cup\mathscr{V}(J)$。

证明 读者自证 1),2),3)．根据 1)，由于

$$I\cap J\subset I,\quad I\cap J\subset J,$$

所以 $\mathscr{V}(I\cap J)\supset\mathscr{V}(I)$，$\mathscr{V}(I\cap J)\supset\mathscr{V}(J)$，即有

$$\mathscr{V}(I\cap J)\supset\mathscr{V}(I)\cup\mathscr{V}(J).$$

又设 $(a_1,\cdots,a_n)\overline{\in}\mathscr{V}(I)\cup\mathscr{V}(J)$，则必有多项式 $f(x_1,\cdots,x_n)\in I$，$g(x_1,\cdots,x_n)\in J$，使

$$f(a_1,\cdots,a_n)\neq 0,\quad g(a_1,\cdots,a_n)\neq 0.$$

显然，$f\cdot g\in I\cap J$，且

$$(f\cdot g)(a_1,\cdots,a_n)=f(a_1,\cdots,a_n)g(a_1,\cdots,a_n)\neq 0,$$

所以 $(a_1,\cdots,a_n)\overline{\in}\mathscr{V}(I\cap J)$。▌

例 7 任给一个理想 I，$\sqrt{I}=$？我们可以用定理6.11（希尔伯特零点定理的强式）来求解答。例如，$I=(x^2,xy)$。先求 $\mathscr{V}(I)$，即 $x^2=0$ 与 $xy=0$ 的公解。容易得出 $\mathscr{V}(I)=y$ 轴。再求 $\mathscr{I}(\mathscr{V}(I))$。显然，它是 (x)。于是

$$\sqrt{I}=\mathscr{I}(\mathscr{V}(I))=(x).$$

习　题

1. 证明定理6.12的1),2),3)以及

(1) $\mathscr{I}(\mathscr{V}(I))\supset I$, $\mathscr{V}(\mathscr{I}(B))\supset B$;

(2) $\mathscr{V}(\mathscr{I}(\mathscr{V}(I)))=\mathscr{V}(I)$, $\mathscr{I}(\mathscr{V}(\mathscr{I}(B)))=\mathscr{I}(B)$,

这里I是理想，B是仿射空间的子集。

2. 设$\mathfrak{a}$和$\mathfrak{b}$是环R的理想。证明

$$\sqrt{\mathfrak{a}}+\sqrt{\mathfrak{b}}=R\Longrightarrow \mathfrak{a}+\mathfrak{b}=R.$$

3. 设有环映射$f: A\to B$。又设$\mathfrak{a}$和$\mathfrak{b}$分别是A和B的理想。证明

(1) $f(\sqrt{\mathfrak{a}})B=\sqrt{f(\mathfrak{a})B}$;

(2) $f^{-1}(\sqrt{\mathfrak{b}})=\sqrt{f^{-1}(\mathfrak{b})}$.

4. 设R是环，I为R的理想。证明$\sqrt{I}$等于包含I的所有素理想的交。

5. 设K是代数封闭域，I是多项式环$K[x_1,x_2,\cdots,x_n]$的理想。证明$\sqrt{I}$是包含I的所有极大理想的交。

6. 在环$\boldsymbol{Z}/m\boldsymbol{Z}$中求$\sqrt{(0)}$，其中$m\in\boldsymbol{Z}$。

7. 找出环$\boldsymbol{Z}/100\boldsymbol{Z}$的所有幂零元和可逆元。

8. 证明$\sqrt{(0)}$是环中所有幂零元的集合。

9. 令

$$I=(x^3-yz,y^2-xz,z^2-x^2y)\subset\boldsymbol{C}[x,y,z],$$

求$\mathscr{V}(I)$。

10. 令

$$I=(x^2+xy,x^3+xy)\subset\boldsymbol{C}[x,y],$$

求$\sqrt{I}$.

11. 设$f,g\in\boldsymbol{C}[x_1,x_2,\cdots,x_n]$，且

$$g(a_1,a_2,\cdots,a_n)=0\Longrightarrow f(a_1,a_2,\cdots,a_n)=0.$$

证明f的素因子都是g的素因子。

12. 设$f(x_1,x_2,\cdots,x_n)$是$\boldsymbol{C}[x_1,x_2,\cdots,x_n]$中的不可约多项

式。证明$\mathscr{V}(f(x_1,x_2,\cdots,x_n))$不能表为两个代数多样体的非平凡并集。

13. 证明$A^n\backslash\{0\}$不是一个代数多样体。

14. 令$V=\{(t,t^2,t^3):t\in C\}\subset A^3$。求$\mathscr{I}(V)\subset C[x_1,x_2,x_3]$。证明$V$不能分解成两个代数多样体的非平凡并集。

§4 环的谱集

在上节中，我们讨论了$K[x_1,\cdots,x_n]$的极大理想。此处K是一个代数封闭域。我们证明了$K[x_1,\cdots,x_n]$中的所有极大理想的集合与n维仿射空间K^n的所有点的集合之间有一个单满映射。对任意的环S，定义其**极大谱集**为

$$\text{mspec}\, S=\{\mathfrak{m}:\mathfrak{m}\text{ 是 }S\text{ 的极大理想}\}.$$

我们可以把mspec S当成点集，而把S当成定义在这个点集上的函数集。具体地说，就是对$f\in S$，$\mathfrak{m}\in\text{mspec}\, S$，令$\tau: S\to S/\mathfrak{m}$为典型映射，则定义

$$f(\mathfrak{m})=\tau(f)\in S/\mathfrak{m}.$$

例 8 令$S=Z$，则$\text{mspec}\,Z=\{(p): p\text{ 为素数}\}$。任取$n\in Z$，则$n$可以考虑成一个函数如下：

$$n((p))=n(\text{mod}\ p)\in Z/(p).$$

当然，这个函数n在不同点(p)的值，属于不同的域$Z/(p)$。这很不同于以前学过的函数。▌

把S作为mspec S上的函数集时，如果有环映射$\sigma: S\to R$，能不能自然地产生一个映射$\sigma^*:\text{mspec}\,R\to\text{mspec}\,S$呢？一般言之，要求函数间的映射与点集间的映射，存在一些自然的对应关系。我们取一个例子：$\sigma: Z\to Q$为嵌入。显然，$\text{mspec}\,Q=\{(0)\}$。$\sigma^*(0)$应是$\sigma^{-1}(0)=(0)\subset Z$。但$(0)\notin\text{mspec}\,Z$。所以，mspec S对映射而言，不是一个自然物。更适当的点集是S的**素谱集**：

$$\text{Spec}\, S=\{\mathfrak{p}:\mathfrak{p}\text{ 是 }S\text{ 的素理想}\}.$$

同样的，我们可以把 S 的元素当成定义在这个点集上的函数，方法如下：对 $f\in S$，$\mathfrak{p}\in\operatorname{Spec}S$，令 $\tau: S\to S_{\mathfrak{p}}\to S_{\mathfrak{p}}/\mathfrak{p}S_{\mathfrak{p}}$，则定义

$$f(\mathfrak{p})=\tau(f)\in S_{\mathfrak{p}}/\mathfrak{p}S_{\mathfrak{p}}.$$

此时，如有环映射 $\sigma: S\to R$，我们定义

$$\sigma^*: \operatorname{Spec}R\to\operatorname{Spec}S,$$
$$\sigma(\mathfrak{q})=\sigma^{-1}(\mathfrak{q})\in\operatorname{Spec}S.$$

在点集 Spec S 上，我们可以定义如下的 Zariski 拓扑，使 Spec S 成为一个拓扑空间。

定理6.13 任给环 S 的理想 I，令

$$\mathscr{V}(I)=\{\mathfrak{p}: \mathfrak{p}\in\operatorname{Spec}S,\ \mathfrak{p}\supset I\}.$$

则我们恒有：

1) $\mathscr{V}((1))=\varnothing$，$\mathscr{V}((0))=\operatorname{Spec}S$；

2) $\bigcap\mathscr{V}(I_i)=\mathscr{V}\left(\sum_i I_i\right)$；

3) $\mathscr{V}(I_1)\cup\mathscr{V}(I_2)=\mathscr{V}(I_1\cdot I_2)$.

因此，我们令 $\mathscr{V}(I)$ 为 Spec S 的闭集，则以上三条保证了这是一个拓扑，称为 Zariski 拓扑。

证明 参考定理6.12，读者自证之。▎

讨论 特别地，当 $S=K[x_1,\cdots,x_n]$ 时，我们把 Spec S 的点（即 S 的素理想）$\mathfrak{p}$ 与它的代数多样体 $\mathscr{V}(\mathfrak{p})$ 对应起来，则 Spec S 的 Zariski 拓扑就给出 n 维仿射空间 K^n 的一个拓扑（即其闭集均为 S 的理想 I 的代数多样体 $\mathscr{V}(I)$），称为 K^n 的 Zariski 拓扑。

例 9 令 $S=\mathbf{C}[x]$，则 $\operatorname{Spec}\mathbf{C}[x]=\{(0)\}\cup\{(x-a): a\in\mathbf{C}\}$。它的几何意义是 (0) 对应于平面 $\mathbf{C}$，$(x-a)$ 对应于点 a。Spec $\mathbf{C}[x]$ 的闭集是什么？我们自然有 $\varnothing$ 及全集合 Spec $\mathbf{C}[x]$。若任取一理想 $I\neq(0),(1)$。令 $I=(f(x))=(\prod(x-a_i))$。则立见

$$\mathscr{V}(I)=\{(x-a_1)\}\cup\{(x-a_2)\}\cup\cdots\cup\{(x-a_n)\},$$

相当于 $\mathbf{C}$ 中的有限个点 $\{a_1,a_2,\cdots,a_n\}$，这就是所有的闭集，请

注意，在一般拓扑下，无限集$\{1,2,\cdots,n,\cdots\}$是一个闭集。可是它在 Zariski 拓扑下并不是一个闭集。

例10 令$S=\boldsymbol{Z}$。则

$$\operatorname{Spec}\boldsymbol{Z}=\{(0)\}\cup\{(p):p\text{ 为素数}\}.$$

任取理想$(n)\neq(0),(1)$，令$n=\prod_{i=1}^{m}p_i^{n_i}$，不难看出

$$\mathscr{V}((n))=\bigcup_{i=1}^{m}\{(p_i)\}.$$

这些有限点集，再加上$\varnothing$及全集合 Spec $\boldsymbol{Z}$，就构成了所有的闭集。

符号 任给 Spec$S$ 的闭集C，以$\mathscr{I}(C)$表示C中所有素理想的交，即

$$\mathscr{I}(C)=\bigcap_{\mathfrak{p}\in C}\mathfrak{p}.$$

定理6.14 任取 $\mathfrak{q}\in\operatorname{Spec}S$。则$\{\mathfrak{q}\}$的闭包为

$$\overline{\{\mathfrak{q}\}}=\{\mathfrak{p}:\mathfrak{p}\supset\mathfrak{q}\}=\mathscr{V}(\mathfrak{q}).$$

证明 显然闭集$\mathscr{V}(\mathfrak{q})\supset\{\mathfrak{q}\}$。设另有闭集$\mathscr{V}(I)\supset\{\mathfrak{q}\}$。任取 $\mathfrak{p}\in\mathscr{V}(\mathfrak{q})$，则有 $\mathfrak{p}\supset\mathfrak{q}\supset I$，即 $\mathfrak{p}\in\mathscr{V}(I)$，$\mathscr{V}(\mathfrak{q})\subset\mathscr{V}(I)$。所以$\overline{\{\mathfrak{q}\}}=\mathscr{V}(\mathfrak{q})$。 ▎

例11 在例 9 中，$\{(x-a)\}$是闭集。$\{(0)\}$不是闭集，它的闭包$\overline{\{(0)\}}=\operatorname{Spec}\boldsymbol{C}[x]$。同理，在例10中，$\{(p)\}$是闭集，$\{(0)\}$不是闭集。它的闭包$\overline{\{(0)\}}=\operatorname{Spec}\boldsymbol{Z}$。

定理6.15 Spec$S$ 是一**拟紧致空间**。这就是说，任给Spec$S$ 的一个开覆盖$\bigcup U_i=\operatorname{Spec}S$，必存在一个有限的子覆盖。

证明 任取 $a\in S$，令 $X_a=\operatorname{Spec}S\backslash\mathscr{V}((a))$。则 Spec S的任意开集U必形如

$$U=\operatorname{Spec}S\backslash\mathscr{V}(I)=\bigcup_{a\in I}\operatorname{Spec}S\backslash\mathscr{V}((a))=\bigcup_{a\in I}X_a.$$

所以

$$\bigcup U_i = \bigcup_{a\in A} X_a,$$

其中A为S的一个子集．令J为A生成的理想，则不难看出

$$\operatorname{Spec} S = \bigcup U_i = \bigcup_{a\in J} X_a = \operatorname{Spec} S\backslash \mathscr{V}(J).$$

于是$\mathscr{V}(J)=\varnothing$，也即$J=(1)$．所以存在$s_1,\cdots,s_m\in S$，使

$$\sum_{i=1}^{m} s_i a_i = 1, \qquad a_i\in A.$$

立得

$$\begin{aligned}\bigcup_{i=1}^{m} X_{a_i} &= \operatorname{Spec} S\backslash \mathscr{V}((a_1,\cdots,a_m))\\ &= \operatorname{Spec} S\backslash \mathscr{V}((1)) = \operatorname{Spec} S.\end{aligned}$$

取出包含X_{a_i}的开集$U_i(i=1,\cdots,m)$，立得

$$\bigcup_{i=1}^{m} U_i = \operatorname{Spec} S. \quad \blacksquare$$

回到原来引出素谱集Spec S的讨论．设有环映射$\sigma: S\to R$，自然得出σ^*: Spec $R\to$Spec S．我们要证明：

定理6.16 设$\sigma: S\to R$是环映射，则σ^*: Spec $R\to$Spec S是连续映射．

证明 任取Spec S的开集$U=\bigcup X_a$（参考上定理的证明），则有

$$(\sigma^*)^{-1}(U) = \bigcup (\sigma^*)^{-1}(X_a).$$

显然，只要证明$(\sigma^*)^{-1}(X_a)$是开集，便足够了．事实上，对于$\mathfrak{q}\in$Spec R，有

$$\mathfrak{q}\not\ni\sigma(a)\Longleftrightarrow\sigma^{-1}(\mathfrak{q})\not\ni a\Longleftrightarrow\sigma^*(\mathfrak{q})\not\ni a.$$

故$(\sigma^*)^{-1}(X_a)=\operatorname{Spec} R\backslash\mathscr{V}(\sigma(a))$为Spec R中的开集．$\blacksquare$

例12 设$i: S\to R$是嵌入．换句话说，S是R的子环．不难看出，任取$\mathfrak{q}\in$Spec R，则

$$i^*(\mathfrak{q}) = i^{-1}(\mathfrak{q}) = \mathfrak{q}\cap S.$$

这相当于几何学上的投影。例如，取

$$S = \boldsymbol{C}[x]\subset \boldsymbol{C}[x,y]/(y^2-x).$$

令 $\mathfrak{q}_1=(x-1,y-1)$，$\mathfrak{q}_2=(x-1,y+1)$，则

$$i^*(\mathfrak{q}_1)=(x-1)=i^*(\mathfrak{q}_2). \quad \blacksquare$$

从点集与函数的关系来考虑 Spec S 与 S，尚有一个问题：S 中可能有**幂零元素** f，即 $f\neq 0$，但 $f^n=0$。一般说来是不准许这样的函数出现的。补救的方法是考虑 S 的**幂零根理想** nil rad(S)，见下面的定理。

定理6.17 1) 令

$$\text{nil rad}(S)=\{f: \text{存在正整数 } n, \text{ 使 } f^n=0\}.$$

则 nil rad(S)是 S 的理想；

2) 令 $I=$nil rad(S)，则 nil rad$(S/I)=(0)$。一般言之，如果 nil rad$(R)=0$，则称 R 是**约化了的**。因此，S/I 是约化了的环。

3) 令 $I=$nil rad(S)，$\sigma: S\to S/I$ 是典型映射，则

$$\sigma^*: \text{Spec}(S/I)\to \text{Spec } S$$

是同胚映射。

证明 1) 设 $f,g\in$nil rad(S)。则有正整数 n,m，使得 $f^n=0$，$g^m=0$。于是

$$(f+g)^{m+n}=\sum_{i=0}^{m+n}\binom{m+n}{i}f^ig^{m+n-i}=0.$$

由此易知 nil rad(S)是一个理想。

2) 令 $\bar{h}\in$nil rad(S/I)，则存在正整数 n，使 $\bar{h}^n=0$，即 $h^n\in I$。所以有正整数 m，使$(h^n)^m=0$。立得 $h\in I$，$\bar{h}=0$。

3) 任取 $\mathfrak{p}\in$Spec S，$f\in I$，则 $f^n=0\in\mathfrak{p}$。因为 $\mathfrak{p}$ 是素理想，所以 $f\in\mathfrak{p}$。于是 $\mathfrak{p}\supset I$。不难看出 $\sigma^*(\mathfrak{p}/I)=\mathfrak{p}$。显然，$\sigma^*$ 是一个同胚映射。 $\blacksquare$

讨论 1) 在我们讨论点集与函数的关系时，常常把环 S 约

化，即以$S/\text{nil rad}(S)$代替S。

2）如果我们讨论微分形式、变形等，环S自然有幂零元素，这是不能由约化来取消的。 ▌

我们在拓扑空间的讨论中，有下面的基本概念。

定义6.8 如果拓扑空间V的闭子集C不能表成它的两个真闭子集C_1,C_2的并集，也即：$C=C_1\cup C_2\Longrightarrow C=C_1$或$C=C_2$，则称$C$为**不可约子集**。$n$维仿射空间$K^n$在Zariski拓扑下的不可约子集称为**不可约代数多样体**。若此代数多样体为代数曲线，则称为**不可约代数曲线**。

讨论 取$V=\mathbf{C}$。如果我们用通常的拓扑，则

$$\mathbf{C}=\{x+iy:\ x\geqslant 0\}\cup\{x+iy:\ x\leqslant 0\}.$$

所以，对于通常的拓扑而言，$\mathbf{C}$不是不可约集。同样地取$V=\mathbf{C}$，可是我们用Zariski拓扑，设$\mathbf{C}=C_1\cup C_2$。由于C_1,C_2只可能是$\varnothing$，$\mathbf{C}$或有限集，不难看出$C_1=\mathbf{C}$或$C_2=\mathbf{C}$。所以$\mathbf{C}$对于Zariski拓扑是不可约的。

定理6.18 设C为$\operatorname{Spec} S$的闭集。则C是不可约子集$\Longleftrightarrow C=\mathscr{V}(\mathfrak{p})$，其中$\mathfrak{p}\in\operatorname{Spec} S$。此时，称$\mathfrak{p}$为$C$的**一般点**。

证明 $\Longrightarrow$。设$C=\mathscr{V}(I')$。令$I=\sqrt{I'}$，则$C=\mathscr{V}(I)$，且$I=\sqrt{I}$。我们来证明I是素理想。假若不然，则存在$f,g\notin I$，但$f\cdot g\in I$。令

$$I_1=I+(f),\qquad I_2=I+(g).$$

则不难看出

$$I\supset I_1\cdot I_2=(I+(f))(I+(g))=I^2+(f)I+(g)I+(fg)\supset I^2.$$

所以

$$\mathscr{V}(I)\subset\mathscr{V}(I_1\cdot I_2)=\mathscr{V}(I_1)\cup\mathscr{V}(I_2)\subset\mathscr{V}(I^2)=\mathscr{V}(I).$$

令$C_1=\mathscr{V}(I_1)$，$C_2=\mathscr{V}(I_2)$，立得$C=C_1\cup C_2$。现在我们要证明$C_1\subsetneqq C$，$C_2\subsetneqq C$（如此，则C是可约的，与已知条件矛盾，也就证明了I是素理想）。因为$I=\sqrt{I}$，$f\notin I$，所以$f^n\notin I$（$n=1,2,\cdots$）。设

$$D=\{f^n: n=1,2,\cdots\},$$

$$\mathscr{F}=\{J: J\text{是理想},\ J\supset I,\ J\cap D=\varnothing\}.$$

不难用Zorn引理证明$\mathscr{F}$中存在一极大元素$\mathfrak{q}$，而且$\mathfrak{q}$是一个素理想(参考定理3.23的证明)。于是$\mathfrak{q}\in C$，$\mathfrak{q}\overline{\in}C_1$，也即$C\supsetneqq C_1$。同样可证$C\supsetneqq C_2$。于是，取$\mathfrak{p}=I$即可。

$\Longleftarrow$。设$C=\mathscr{V}(\mathfrak{p})=C_1\cup C_2$，其中

$$C_1=\mathscr{V}(I_1)\neq C,\qquad C_2=\mathscr{V}(I_2)\neq C.$$

显然，$I_1\supsetneqq\mathfrak{p}$，$I_2\supsetneqq\mathfrak{p}$。令$f\in I_1\backslash\mathfrak{p}$，$g\in I_2\backslash\mathfrak{p}$，则有

$$\mathfrak{p}\in\mathscr{V}(\mathfrak{p})=\mathscr{V}(I_1)\cup\mathscr{V}(I_2)=\mathscr{V}(I_1\cdot I_2).$$

于是$\mathfrak{p}\supset I_1\cdot I_2\ni f\cdot g$。这是不可能的。▌

一般在代数学里，我们极有兴趣的是S为诺德环的情形。为此，我们引入“诺德空间”的概念。

定义6.9 设V为一个拓扑空间。如果任给的闭子集的链

$$C_1\supset C_2\supset\cdots\supset C_n\supset\cdots$$

经过有限步以后，必然终了，即存在m，使$n\geqslant m$时，必有$C_n=C_{n+1}$，则称V为**诺德空间**。

我们有下面的定理。

定理6.19 1）如果S是诺德环，则Spec S是诺德空间；

2）如果V是诺德空间，则V的任意的闭子集C可以唯一地分解成互不包含的不可约子集C_i的并集：

$$C=C_1\cup C_2\cup\cdots\cup C_n,\qquad C_i\not\supset C_j\quad(i\neq j).$$

证明 1）令$I_i=\mathscr{I}(C_i)$，则我们从Spec S的任一闭子集的链

$$C_1\supset C_2\supset\cdots\supset C_n\supset\cdots$$

导出S中的理想链

$$I_1\subset I_2\subset\cdots\subset I_n\subset\cdots.$$

因为S是诺德环，所以存在m，使$n\geqslant m$时，必有$I_n=I_{n+1}$，即有$C_n=\mathscr{V}(I_n)=\mathscr{V}(I_{n+1})=C_{n+1}$。

2）如果C是不可约子集，则令$C=C$。如果C是可约子集，

则存在闭子集 C_1, C_2，使

$$C = C_1 \cup C_2, \quad C \supsetneqq C_1, \quad C \supsetneqq C_2.$$

如果 C_1, C_2 都是不可约子集，则上式即是一个分解式。否则，不妨设 C_1 是可约子集。令 $C_1 = C_{11} \cup C_{12}$。如此程序可以一直作下去。如果始终得不到不可约子集分解式，则有

$$C \supsetneqq C_1 \supsetneqq \cdots.$$

这与 V 是诺德空间的条件相违。这样，我们证明了分解的存在性。

以下证明分解的唯一性。设有

$$C = C_1 \cup C_2 \cup \cdots \cup C_n = C'_1 \cup C'_2 \cup \cdots \cup C'_m,$$

其中 C_i, C'_i 均为不可约子集，且 $C_i \not\supset C_j$，$C'_i \not\supset C'_j$ $(i \neq j)$。我们有

$$C_1 = C_1 \cap C = \sum_{i=1}^{m} (C_1 \cap C'_i).$$

因为 C_1 是不可约子集，所以必存在 i，使

$$C_1 = C_1 \cap C'_i, \quad C_1 \subset C'_i.$$

同法可证存在 j，使 $C'_i \subset C_j$。于是

$$C_1 \subset C'_i \subset C_j.$$

所以必有 $1 = j$，$C_1 = C'_i$。依次证明，不难看出，除了次序不同外，此二分解是完全一样的。▌

系 设 S 是诺德环，I 是理想，$I = \sqrt{I}$。则我们恒有

$$I = \bigcap_{i=1}^{n} \mathfrak{p}_i,$$

其中 $\mathfrak{p}_i$ 是素理想，$\mathfrak{p}_i \not\subset \mathfrak{p}_j$。而且上式除了 $\mathfrak{p}_i$ 的次序外，是由 I 唯一确定的。

证明 令 $C = \mathscr{V}(I)$。由上面的定理，存在 $\operatorname{Spec} S$ 中的不可约子集 C_i，使

$$C=\bigcup_{i=1}^{n}C_i,\quad C_i\not\supset C_j\quad(i\neq j),$$

且此分解是唯一的。设$C_i=\mathscr{V}(\mathfrak{p}_i)$，$\mathfrak{p}_i$为$S$的素理想。则立得

$$C=\sum_{i=1}^{n}\mathscr{V}(\mathfrak{p}_i)=\mathscr{V}\left(\bigcap_{i=1}^{n}\mathfrak{p}_i\right).$$

于是
$$I=\mathscr{I}(C)=\mathscr{I}\left(\mathscr{V}\left(\bigcap_{i=1}^{n}\mathfrak{p}_i\right)\right)=\bigcap_{i=1}^{n}\mathfrak{p}_i.$$

易见此分解也是唯一的。∎

例13 取$f(x,y)=x^2(y-x^2)$。令$C=\mathscr{V}((f))$，则

$$C=\mathscr{V}(\sqrt{(f)})=\mathscr{V}((x(y-x^2)))$$
$$=\mathscr{V}((x))\cup\mathscr{V}((y-x^2)),$$

即C是$x=0$（y轴)及$y-x^2=0$（抛物线)的并集。令$I=\sqrt{(f)}=(x(y-x^2))$，则有

$$I=(x)\cap(y-x^2),$$

即I分解成两个素理想的交集。∎

将定理6.19的结论2）翻译成n维仿射空间K^n中的语言(参考定义6.8)，即有

定理6.19′ n维仿射空间K^n中的任一代数多样体可唯一分解成互不包含的不可约代数多样体的并集。

习　题

1．设R是环．证明$\operatorname{Spec}R$是T_0空间(即对$\mathfrak{p}_1,\mathfrak{p}_2\in\operatorname{Spec}R$，$\mathfrak{p}_1\neq\mathfrak{p}_2$，必存在一个开集含有$\mathfrak{p}_1$但不含$\mathfrak{p}_2$，或者含有$\mathfrak{p}_2$但不含$\mathfrak{p}_1$)。

2．设S是环．任取$a\in S$，令$X_a=\operatorname{Spec}(R)\backslash\mathscr{V}((a))$。证明当$a$是幂等元(即$a^2=a$)时，$X_a$是开集也是闭集。

3．证明$\operatorname{Spec}S$是连通的$\Longleftrightarrow S$的幂等元只有0和1．

4．证明$\operatorname{Spec}S$是不可约的$\Longleftrightarrow\sqrt{(0)}$是素理想。

5. 证明 Spec S（在包含关系下的）极大的不可约子集是形如 $\mathscr{V}(\mathfrak{p})$ 的闭集，这里 $\mathfrak{p}$ 为 S 的极小素理想。

6. 设 $\sigma: S\to R$ 是环映射。σ 诱导出

$$\sigma^*: \operatorname{Spec} R\to \operatorname{Spec} S.$$

如果 σ 是满射，证明

$$\sigma^*(\operatorname{Spec} R)=\mathscr{V}(\ker\sigma),$$

且 σ^* 是到象集的同胚映射。

7. 设 $\mathfrak{p}$ 是环 R 的一个素理想，$f: R\to R_{\mathfrak{p}}$ 是认同映射。f 诱导出 $f^*: \operatorname{Spec} R_{\mathfrak{p}}\to\operatorname{Spec} R$. 证明 $f^*(\operatorname{Spec} R_{\mathfrak{p}})$ 等于在 Spec R 中 $\mathfrak{p}$ 的所有开邻域的交。

8. 找出 Spec $\boldsymbol{C}[x]$ 的所有闭集。

9. 找出 Spec $\boldsymbol{C}[x,y]$ 的所有闭集。

10. 证明 Spec $\boldsymbol{C}[x,y]$ 不与 Spec $\boldsymbol{C}[x]\times$ Spec $\boldsymbol{C}[y]$ 同胚。把 $\boldsymbol{C}[x],\boldsymbol{C}[y]$ 对应到 $\boldsymbol{C}^1$，把 $\boldsymbol{C}[x,y]$ 对应到 $\boldsymbol{C}^2$，考虑上面结论的几何意义。

11. 找出 $\boldsymbol{C}[x,y]/(xy-1)$ 的素谱空间的所有闭集。

12. 设 R 是局部环，找出 $R[[x]]$ 的所有极大理想。

13. 在 $\boldsymbol{C}[x,y,z]$ 中将 $\sqrt{(x^2(y^2-1),xz^2)}$ 分解成素理想的交。

§5 理想的分解

在上一节中，我们讨论了在任意诺德空间 V 里，任意的闭子集 C 分解成不可约子集 C_i 的并集。相应地，在诺德环 S 中，如果理想 $I=\sqrt{I}$，则 $I=\bigcap\mathfrak{p}_i$，$\mathfrak{p}_i$ 是素理想。在本节中，我们将讨论任意理想 I 的分解。

定义6.10 1）设理想 I 不能表成 $I=\bigcap_{i=1}^{n}I_i$，其中 $I_i\supsetneqq I$，则称 I 为**不可约理想**；

2）设理想 I 有下列性质，则称 I 为**准素理想**：$ab\in I$，$a\notin$

$I \Longrightarrow$ 存在正整数 n，使 $b^n \in I$。

讨论 1）如果 I 是准素理想，考虑 $\sqrt{I}$。如果 $ab \in \sqrt{I}$，$a \bar{\in} \sqrt{I}$。则 $a^m b^m = (ab)^m \in I$，$a^m \bar{\in} I$。所以 $(b^m)^l \in I$，即 $b \in \sqrt{I}$。因此我们得出 $\sqrt{I}$ 是一个素理想。

2）反之，如果 $\sqrt{I}$ 是素理想，则 I 不一定是准素理想。例如，取 $I = (x^2, xy) \subset \mathbf{C}[x, y]$。不难看出，$\sqrt{I} = (x)$ 是素理想。但 $x \cdot y \in I$，$x \bar{\in} I$，$y^n \bar{\in} I$（$\forall n = 1, 2, \cdots$），所以 I 不是一个准素理想。

3）一个素理想必然是一个准素理想。

4）一个素理想必然是一个不可约理想。事实上，设 $\mathfrak{p}$ 为素理想，$\mathfrak{p} = I_1 \cap I_2$。假若 $I_1 \supsetneqq \mathfrak{p}$，$I_2 \supsetneqq \mathfrak{p}$，取 $f \in I_1 \setminus \mathfrak{p}$，$g \in I_2 \setminus \mathfrak{p}$，则 $f, g \bar{\in} \mathfrak{p}$，但 $fg \in I_1 \cap I_2 = \mathfrak{p}$。这与 $\mathfrak{p}$ 是素理想相违。

5）一个准素理想 I 不一定是一个不可约理想。例如，令

$$I = (x^2, xy, y^2) \subset \mathbf{C}[x, y].$$

读者自证 I 是一个准素理想。可是 $I = (I + (x)) \cap (I + (y))$，$x \bar{\in} I$，$y \bar{\in} I$。所以 I 不是一个不可约理想。

引理 1）令 S 是诺德环，则任意的一个理想 I，都可以写成 $I = \bigcap_{i=1}^{n} I_i$，其中 I_i 是不可约理想；

2）令 S 是诺德环，I 是不可约理想，则 I 是准素理想。

证明 1）我们应用"极大原则"（参考定理3.25）。令

$$\mathscr{F} = \left\{ I : I \text{ 不能写成 } \bigcap_{i=1}^{n} I_i,\ I_i \text{ 为不可约理想} \right\}.$$

假若 $\mathscr{F} \neq \varnothing$，令 I 是 $\mathscr{F}$ 的极大元，$I = I_1 \cap I_2$，$I_1 \supsetneqq I$，$I_2 \supsetneqq I$。则 $I_1, I_2 \bar{\in} \mathscr{F}$。所以 I_1, I_2 可以写成

$$I_1 = \bigcap_{i=1}^{n} I_{1i}, \qquad I_2 = \bigcap_{i=1}^{m} I_{2i},$$

其中 I_{1i}, I_{2i} 都是不可约理想。我们立得

$$I = \left(\bigcap_{i=1}^{n} I_{1i} \right) \cap \left(\bigcap_{i=1}^{m} I_{2i} \right) \bar{\in} \mathscr{F}.$$

这是自相矛盾的结论，所以 $\mathscr{F}=\varnothing$。

2) 假设 I 不是准素理想，则存在 a,b，使得 $ab\in I$，$a\overline{\in} I$，$b^n\overline{\in} I(\forall n=1,2,\cdots)$。考虑如下定义的集合：

$$J_n=\{c\in S: cb^n\in I\}=I:(b^n).$$

不难看出，J_n 是一个理想，而且有

$$J_1\subset J_2\subset\cdots\subset J_n\subset\cdots.$$

因为 S 是诺德环，所以必存在 m，使 $n\geqslant m$ 时，$J_n=J_{n+1}$。我们先证 $I=(I+(b^m))\cap(I+(a))$。显然

$$I\subset(I+(b^m))\cap(I+(a)).$$

反之，任取 $c\in(I+(b^m))\cap(I+(a))$，则有

$$c=i_1+d_1b^m=i_2+d_2a,\quad i_1\in I,\ i_2\in I,\ d_1,d_2\in S.$$

上式乘以 b，由于 $ab\in I$，我们得

$$d_1b^{m+1}\in I\Longrightarrow d_1\in J_{m+1}=J_m\Longrightarrow d_1b^m\in I$$
$$\Longrightarrow c=i_1+d_1b^m\in I.$$

所以 $I=(I+(b^m))\cap(I+(a))$。又显然 $I+(b^m)\supsetneqq I$，$I+(a)\supsetneqq I$，于是 I 是可约理想。❙

上面的引理说明了，诺德环 S 的任意理想 I 都可以分解成

$$I=\bigcap_{i=1}^{n}I_i,$$

其中 I_i 是准素理想。对于这样的分解式，我们还要稍加整理：1）如果 $I_i\supset\bigcap_{j\neq i}I_j$，我们可以弃去 I_i；2）如果 $\sqrt{I_i}=\sqrt{I_j}$，则可以证明 $I_i\cap I_j$ 也是一个准素理想（设有 $ab\in I_i\cap I_j$，$a\overline{\in} I_i\cap I_j$，不妨设 $a\overline{\in} I_i$，则 $b^n\in I_i$，$b\in\sqrt{I_i}=\sqrt{I_j}$，$b^m\in I_j$，故 $b^{m+n}\in I_i\cap I_j$）。此时，可令 $I_k=I_i\cap I_j$，以取代 $I_i\cap I_j$。

根据上面的讨论，我们可以引入：

定义6.11 一个准素分解 $I=\bigcap_{i=1}^{n}I_i$，如果适合下面的条件，则称为 I 的简略准素分解：

1) $I_i \not\supset \bigcap_{j\neq i} I_j$, $\forall i=1,\cdots,n$;

2) $\sqrt{I_i}\neq\sqrt{I_j}$, $\forall i\neq j$.

定理6.20 设 S 是诺德环，则任意的理想 I 都有一个简略准素分解。

证明 读者自证之。▌

例14 设 $S=\boldsymbol{Z}\ni n=\prod p_i^{m_i}$. 则不难看出 $(n)=\bigcap(p_i^{m_i})$. 反之，$\boldsymbol{Z}$ 的非零准素理想都是形如$(p_i^{m_i})$，此处 p_i 是素数. 因此，任给 $\boldsymbol{Z}$ 的一个理想$(n)\neq(0)$，都可以写成

$$(n)=\bigcap(p_i^{m_i})=\prod(p_i^{m_i}).$$

所以上面的定理在 $S=\boldsymbol{Z}$ 时，相当于整数的分解定理. 可是，一般言之，简略准素分解并不是唯一的. 我们试举一例说明之. 令 $I=(x^2,xy)\subset\boldsymbol{R}[x,y]$. 它定义了 y 轴及原点$(0,0)$(二重). I 的简略分解可写为:

$$I=(x)\cap(y-ax,x^2).$$

前一个理想(x)定义了 y 轴，后一个理想$(y-ax,x^2)$ 定义了一条斜线$(y-ax=0)$与 y 轴相交两次$(x^2=0)$. 显然，$(y-ax,x^2)$ 随 a 的值而变，所以不是唯一的. 请注意，(x)及$\sqrt{(y-ax,x^2)}=(x,y)$是唯一的. 这是下面要讨论的"唯一性定理"的要义.

定理6.21 设 S 是环，它的一个理想 I 的简略准素分解为

$$I=\bigcap_{i=1}^{n} I_i.$$

令$\mathfrak{p}_i=\sqrt{I_i}$ $(i=1,\cdots,n)$，则$\{\mathfrak{p}_i\}$是由 I 唯一确定的.

证明 我们考虑下面的理想

$$I:(c)=\{a\in S:\ ac\in I\}.$$

1) 如果 $c\in I$，自然得出 $I:(c)=S$. 2) 一般言之，不难看出

$$I:(C)=\left(\bigcap_{i=1}^{n} I_i\right):(c)=\bigcap_{i=1}^{n}(I_i:(c)),$$

$$\sqrt{I:(c)}=\sqrt{\bigcap (I_i:(c))}=\bigcap\sqrt{I_i:(c)}.$$

我们指出，当 $c\bar{\in} I_i$ 时，恒有

$$\sqrt{I_i:(c)}=\mathfrak{p}_i.$$

证法如下：设 $a^m\in I_i:(c)$，即 $a^m c\in I_i$。而 $c\bar{\in} I_i$，故有

$$a^{ml}\in I_i\subset\mathfrak{p}_i,$$

所以 $a\in\mathfrak{p}_i$。反之，设 $a\in\mathfrak{p}_i$，则 $a^m\in I_i$，于是

$$a^m c\in I_i,\quad a^m\in I_i:(c),\quad a\in\sqrt{I_i:(c)}.$$

3）当我们取 $c\in\left(\bigcap\limits_{j\neq i} I_j\right)\Big\backslash I_i$ 时，就有 $\sqrt{I:(c)}=\mathfrak{p}_i$。

综上所述，在集合 $\{\sqrt{I:(c)}:\ c\in S\}$ 中，所有的素理想 $\mathfrak{p}_i$ 都出现了。反之，设

$$\mathfrak{p}\in\{\sqrt{I:(c)}:\ c\in S\},$$

则根据 2），必有 $\mathfrak{p}\supset\bigcap\limits_{i=1}^{n}\mathfrak{p}_i$。我们要说明，$\mathfrak{p}$ 必是 $\{\mathfrak{p}_i\}$ 中的某一个。如若不然，则 $\mathfrak{p}_i\supsetneqq\mathfrak{p}(\forall i)$。令 $a_i\in\mathfrak{p}_i\backslash\mathfrak{p}$，则有

$$\prod a_i\in\bigcap\mathfrak{p}_i\subset\mathfrak{p}.$$

这是不可能的。归结来说，$\{\mathfrak{p}_i\}$ 是 $\{\sqrt{I:(c)}:\ c\in S\}$ 中的素理想的集合，因此是由 I 唯一确定的。▎

上面定理中那些由 I 唯一确定的素理想称为"I 的素理想"。$\{\mathfrak{p}_i\}$ 中的极小元称为 I 的**孤立素理想**，其余的称为 I 的**嵌入素理想**。例如，在例14 中，$I=(x^2,xy)$，$\mathfrak{p}_1=(x)$，$\mathfrak{p}_2=(x,y)$。$\mathfrak{p}_1$ 是孤立素理想，$\mathfrak{p}_2$ 是嵌入素理想。从几何学的观点，比较容易理解这些术语：$\mathfrak{p}_1$ 相当于 y 轴，$\mathfrak{p}_2$ 相当于嵌入 y 轴的原点。应用上面的观点，在简略准素分解 $I=\bigcap I_i$ 中，如果 $\sqrt{I_i}=\mathfrak{p}_i$ 是 I 的孤立素理想，则称 I_i 是 I 的**孤立准素分支**；否则，则称 I_i 是 I 的**嵌入准素分支**。我们有下面的唯一性定理。

定理6.22 设 S 是环，它的一个理想 I 的简略准素分解为

$$I=\bigcap_{i=1}^{n} I_i.$$

则 I 的孤立准素分支是由 I 唯一确定的

证明 任取 I_i，令

$$\mathfrak{q}_i = \{x: I:(x) \not\subset \sqrt{I_i}\}.$$

1) 如果 $a \in \mathfrak{q}_i$，即 $I:(a) \not\subset \sqrt{I_i}$，于是存在 $c \bar{\in} \sqrt{I_i}$，$c \in I:(a)$。也即 $ca \in I \subset I_i$，立得 $a \in I_i$。我们证明了 $\mathfrak{q}_i \subset I_i$。2) $\mathfrak{q}_i$ 是一个理想。事实上，若 $a \in \mathfrak{q}_i$，则不难看出，对于任意的 $b \in S$，$ab \in \mathfrak{q}_i$；又若 $a_1, a_2 \in \mathfrak{q}_i$，即存在 $c_1, c_2 \bar{\in} \sqrt{I_i}$，使 $c_1a_1, c_2a_2 \in I$，于是 $c_1c_2 \bar{\in} \sqrt{I_i}$，$c_1c_2(a_1 + a_2) \in I$，也就是说 $a_1 + a_2 \in \mathfrak{q}_i$。因此 $\mathfrak{q}_i$ 是一个理想。3) 当 $\sqrt{I_i}$ 是 I 的孤立素理想时，$\mathfrak{q}_i = I_i$。事实上，根据 1)，恒有 $\mathfrak{q}_i \subset I_i$，所以仅须证明 $\mathfrak{q}_i \supset I_i$。由于 $\mathfrak{p}_i = \sqrt{I_i}$ 是 I 的素理想中的极小者，所以 $\mathfrak{p}_j \not\subset \mathfrak{p}_i (\forall j \neq i)$。取 $b_j \in \mathfrak{p}_j \backslash \mathfrak{p}_i$，设 $b_j^{m_j} \in I_j$，则

$$b = \prod_{j \neq i} b_j^{m_j} \bar{\in} \mathfrak{p}_i = \sqrt{I_i}.$$

显然，对任意的 $a \in I_i$，我们恒有 $ab \in \bigcap I_i = I$，故 $a \in \mathfrak{q}_i$，即有 $I_i \subset \mathfrak{q}_i$。4) 根据定理6.21，易知 I 的孤立素理想 $\mathfrak{p}_i = \sqrt{I_i}$ 是由 I 唯一确定的，再根据 $\mathfrak{q}_i$ 的定义，知 $I_i = \mathfrak{q}_i$ 也是由 I 唯一确定的。▎

讨论 1) 本节的定理是所谓"存在性定理"，而非"构造性定理"，即没有提供一个方法，能实际作出这些简略准素分解等等。

2) 这些定理一般称为 Lasker-Noether **定理**。

3) 熟习本节后，很容易推广到"诺德模的准素分解"理论。

4) 我们考虑 $\text{nil rad}(S) = \sqrt{(0)}$（见定理6.17）的简略准素分解。因为

$$\sqrt{\text{nil rad}(S)} = \sqrt{\sqrt{(0)}} = \sqrt{(0)} = \text{nil rad}(S),$$

所以（参看定理6.19的系）

$$\sqrt{(0)} = \bigcap_{i=1}^{n} \mathfrak{p}_i,$$

此处$\mathfrak{p}_i$都是素理想. 由分解的唯一性，立刻可以看出$\mathfrak{p}_i$都是极小素理想(即任一素理想$\mathfrak{p}\subset\mathfrak{p}_i$，则$\mathfrak{p}=\mathfrak{p}_i$)。另一方面，设$\mathfrak{p}$是一个极小素理想，则有

$$\mathfrak{p}\ni 0\Longrightarrow\mathfrak{p}\supset\sqrt{(0)}=\bigcap_{i=1}^{n}\mathfrak{p}_i$$

$$\Longrightarrow\text{对某个 } i\text{，}\mathfrak{p}\supset\mathfrak{p}_i\Longrightarrow\mathfrak{p}=\mathfrak{p}_i.$$

所以，我们得知在诺德环S里，只有有限多个极小素理想，以及幂零根理想是所有极小素理想的交，也即是所有素理想的交。

5) 以D表示诺德环S中所有零因子构成的集合：

$$D=\{a:\ a\in S,\ \text{存在 } b\in S,\ b\neq 0,\ \text{使} ab=0\}.$$

则我们有

$$\bigcup_{\text{极小素理想}}\mathfrak{p}_i=D.$$

证明如下：令$(0)=\bigcap I_i$是简略准素分解，$\sqrt{I_i}=\mathfrak{p}_i$，则$\mathfrak{p}_i$为极小素理想。参看定理6.21的证明，对每个极小素理想$\mathfrak{p}_i$，都存在$c\neq 0$，使$\mathfrak{p}_i=\sqrt{(0):(c)}$。所以，任取$a\in\mathfrak{p}_i$，$a\neq 0$，必存在正整数$r$，使$a^r c=0$。取满足此式的最小的$r$，则有$a(a^{r-1}c)=0$，$a^{r-1}c\neq 0$。故$\mathfrak{p}_i\subset D$。即有$\bigcup\mathfrak{p}_i\subset D$。反之，由于

$$(0):(a)=\{b:\ ba=0\},$$

所以

$$D=\{a:\ (0):(a)\neq(0)\}.$$

设$a\in D$，则存在$b\in(0):(a)$，$b\neq 0$。于是$a\in(0):(b)$，$b\neq 0$。故

$$D\subset\bigcup_{b\neq 0}((0):(b))\subset\bigcup_{b\neq 0}\sqrt{(0):(b)}=\bigcup\mathfrak{p}_i.$$

习　题

1. 设R是环，$\mathfrak{a},\mathfrak{b},\mathfrak{c},\mathfrak{a}_i,\mathfrak{b}_i$是$R$的理想。证明

(1) $\mathfrak{a}\subset\mathfrak{a}:\mathfrak{b}$；　　(2) $(\mathfrak{a}:\mathfrak{b})\cdot\mathfrak{b}\subset\mathfrak{a}$；

(3) $(\mathfrak{a}:\mathfrak{b}):\mathfrak{c}=\mathfrak{a}:\mathfrak{b}\mathfrak{c}=(\mathfrak{a}:\mathfrak{c}):\mathfrak{b}$;

(4) $(\bigcap\mathfrak{a}_i):\mathfrak{b}=\bigcap(\mathfrak{a}_i:\mathfrak{b})$;

(5) $\mathfrak{a}:\left(\sum_i\mathfrak{b}_i\right)=\bigcap(\mathfrak{a}:\mathfrak{b}_i)$.

2. 设有环同态 $f: R\to S$，$\mathfrak{a}_1,\mathfrak{a}_2$ 是 R 的理想，$\mathfrak{b}_1,\mathfrak{b}_2$ 是 S 的理想。证明：

(1) $f(\mathfrak{a}_1:\mathfrak{a}_2)S\subset(f(\mathfrak{a}_1)S):(f(\mathfrak{a}_2)S)$;

(2) $f^{-1}(\mathfrak{b}_1:\mathfrak{b}_2)\subset f^{-1}(\mathfrak{b}_1):f^{-1}(\mathfrak{b}_2)$.

3. 证明 $I_1:I_2=I_1\Longleftrightarrow I_2$ 不含于 I_1 的任何素理想之中。

4. 设 $\mathfrak{p}$ 为环 R 的素理想，$\mathfrak{a},\mathfrak{b}$ 为理想，且 $\mathfrak{a}\mathfrak{b}\subset\mathfrak{p}$。如果 $\mathfrak{a}\not\subset\mathfrak{p}$，证明 $\mathfrak{b}\subset\mathfrak{p}$。

5. 设 $\mathfrak{q}$ 为 R 的准素理想，$\mathfrak{a},\mathfrak{b}$ 为理想，且 $\mathfrak{b}$ 是有限生成的。如果 $\mathfrak{a}\mathfrak{b}\subset\mathfrak{q}$，但 $\mathfrak{a}\not\subset\mathfrak{q}$，证明存在正整数 n，使得 $\mathfrak{b}^n\subset\mathfrak{q}$。

6. 设 S 是环，$\mathfrak{q}$ 为 S 的准素理想，$\sqrt{\mathfrak{q}}=\mathfrak{p}$。令

$$\mathfrak{q}^{(n)}=\mathfrak{q}^nS_{\mathfrak{p}}\cap S.$$

称 $\mathfrak{q}^{(n)}$ 为 $\mathfrak{q}$ 的符号方幂(symbolic power)。证明 $\mathfrak{q}^{(n)}$ 是 S 的准素理想，且 $\sqrt{\mathfrak{q}^{(n)}}=\mathfrak{p}$。

7. 举例说明以素理想 $\mathfrak{p}$ 为根的无穷多个准素理想的交不一定是以 $\mathfrak{p}$ 为根的准素理想。

8. 设 K 是域。证明在多项式环 $K[x_1,x_2,\cdots,x_n]$ 中理想

$$\mathfrak{p}_i=(x_1,x_2,\cdots,x_i)\quad(i=1,2,\cdots,n)$$

都是素理想，它们的方幂都是准素理想。

9. 令 $I=\bigcap I_i$ 是环 S 的理想的简略准素分解，$\sigma: S\to S/I$ 是典型映射。证明

$$(0)=\bigcap\sigma(I_i)\subset S/I$$

是 (0) 在 S/I 中的简略准素分解。反之，令

$$(0)=\bigcap I_i\subset S/I$$

是 (0) 在 S/I 的简略准素分解，证明

$$I=\bigcap\sigma^{-1}(I_i)\subset S$$

是 I 的一个简略准素分解。

10. 设有环满射 $f: R \to S$。设 $\mathfrak{q}$ 是 S 的理想。证明

(1) $\mathfrak{q}$ 是 S 的准素理想当且仅当 $f^{-1}(\mathfrak{q})$ 是 R 的准素理想;

(2) $\mathfrak{q}$ 是以 $\mathfrak{p}$ 为根的准素理想，则 $f^{-1}(\mathfrak{q})$ 以 $f^{-1}(\mathfrak{p})$ 为根。

11. 设 R 是环，x 是变元。证明

(1) 如果 $\mathfrak{p}$ 是 R 的素理想，则 $\mathfrak{p}[x]$ 是 $R[x]$ 的素理想;

(2) 如果 $\mathfrak{q}$ 是 R 中的 $\mathfrak{p}$ 准素理想(即 $\sqrt{\mathfrak{q}} = \mathfrak{p}$，$\mathfrak{q}$ 准素)，则 $\mathfrak{q}[x]$ 是 $R[x]$ 中的 $\mathfrak{p}[x]$ 准素理想;

(3) 如果 $\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i$ 是 $\mathfrak{a}$ 在 R 中的一个简略准素分解，则 $\mathfrak{a}[x] = \bigcap_{i=1}^{n} \mathfrak{q}[x]$ 是 $R[x]$ 中的简略准素分解;

(4) 如果 $\mathfrak{p}$ 是 R 的极小素理想，则 $\mathfrak{p}[x]$ 是 $R[x]$ 的极小素理想。

12. 设 F 为任一域。在 $F[x, y]$ 中，令 $\mathfrak{a} = (x^2, xy)$，证明下述分解都是简略准素分解:

(1) $\mathfrak{a} = (x) \cap (x^2, y)$;　　(2) $\mathfrak{a} = (x) \cap (x^2, x+y)$;

(3) $\mathfrak{a} = (x) \cap (x^2, xy, y^2)$。

13. 令 $I = (x^2 + y^2 - 1, xy - 1) \subset \mathbf{C}[x, y]$。找出 I 的简略准素分解。

14. (I.S.Cohen) 证明 S 是诺德环 $\Longleftrightarrow$ S 的每个素理想都是有限生成的。

15. 平行于环的准素分解，建立模的准素分解的理论。

§6 维数论(1)

一个拓扑空间的基本性质之一是它的维数。一般言之，我们有许多不同的方式来讨论维数，现列举几条如下。

1) 空间的自由度。直观来说，n 维仿射空间 $\mathbf{A}^n$ 的维数应

该是 n。如果有 $\sigma: V \to \boldsymbol{A}^n$ 是一个满射，而且映射 σ 的纤维 $\sigma^{-1}(a)$ 都是有限集，则我们定义 V 的维数应当同于 $\boldsymbol{A}^n$ 的维数 n。请参考定理6.8。以后我们将详细讨论之。

2）如果拓扑空间的任何一个开覆盖 $\cup U_i$ 都可细化成一个开覆盖 $\cup V_j$(即 $V_j \subset U_i$)，使任何 $n+2$ 个 V_j 的交都是空集 $\varnothing$，这种 n 的最小可能的正整数值称为空间 V 的维数。例如，我们取 $V=\boldsymbol{R}$，即一条直线。不难看出，任给一个开覆盖 $\cup U_i$(只要不是用 V 作自身的开覆盖)，不可避免地会有两个开集的交集非空。而适当地加细 $\cup U_i$ 以后，可以使得任何三个新的开集的交为空集。所以，在这种定义下，$\boldsymbol{R}$ 的维数是1。同样的，$\boldsymbol{R}^n$ 的维数是 n。本节中，我们将不讨论这种维数。

3）在诺德空间里，我们定义闭点的维数是零。如果一个不可约子集 $B \supsetneqq$ 不可约子集 C，而且在 B，C 间不能插入任何不可约子集，则我们定义

$$\dim B = \dim C + 1,$$

即 B 的维数 $=C$ 的维数 $+1$。例如，平面上有直线，直线上有点，因此，我们认为平面的维数是2，直线的维数是1。

我们先把3)精确化，得出下面的定义。

定义6.12 设 S 是一个诺德环。S 的 Krull 维数 $\dim S$ 定义为 S 的素理想链 $\mathfrak{p}_0 \supsetneqq \mathfrak{p}_1 \supsetneqq \cdots \supsetneqq \mathfrak{p}_n$ 的长度 n 的最大值。如果这个最大值不存在，则定义 $\dim S=\infty$。

讨论 在一个诺德环 S 里，任何一个素理想的链都只有有限的长度，但是它们的长度可能越来越长，趋向于无限大。因此，可能有 $\dim S=\infty$。永田雅宜在他的书"Local Ring"的附录中，提供了一个实例。▎

与定理6.9(Cohen 及 Seidenberg 上升定理）相结合，我们有下面的定理。

定理6.23 设环 R 是对环 S 整数相关的（即每一个 $r \in R$ 都是对 S 整数相关的），$R \supset S$。则恒有

$$\dim R = \dim S.$$

证明 任取S的一个素理想的链

(1) $$\mathfrak{p}_0 \supsetneqq \mathfrak{p}_1 \supsetneqq \cdots \supsetneqq \mathfrak{p}_n,$$

应用定理6.9后面的讨论，我们立得R的一个素理想的链

(2) $$\mathfrak{q}_0 \supsetneqq \mathfrak{q}_1 \supsetneqq \cdots \supsetneqq \mathfrak{q}_n, \quad \mathfrak{q}_i \cap S = \mathfrak{p}_i.$$

所以 $\dim R \geqslant \dim S$。反之，任取R的素理想的链(2)，令$\mathfrak{q}_i \cap S = \mathfrak{p}_i$。仅须证明

$$\mathfrak{q}_i \supsetneqq \mathfrak{q}_{i+1} \Longrightarrow \mathfrak{p}_i \supsetneqq \mathfrak{p}_{i+1},$$

便足以证明

$$\dim S \geqslant \dim R.$$

令 $R' = R/\mathfrak{q}_{i+1}$，$\mathfrak{q}'_i = \mathfrak{q}_i/\mathfrak{q}_{i+1}$，$S' = S/\mathfrak{p}_{i+1}$，$\mathfrak{p}'_i = \mathfrak{p}_i/\mathfrak{p}_{i+1}$。显然，$R' \supset S'$，$R'$ 对 S' 是整数相关的。于是，问题归结为：

$$\mathfrak{q}'_i \neq (0) \Longrightarrow \mathfrak{p}'_i = \mathfrak{q}'_i \cap S' \neq (0).$$

任取 $r \in \mathfrak{q}'_i$，$r \neq 0$。令 $f(x) \in S'[x]$ 为 r 适合的最低次数的首一多项式。写出 $f(x)$如下：

$$f(x) = x^n + s_1 x^{n-1} + \cdots + s_n, \quad s_i \in S'.$$

则 $s_n \neq 0$。这是因为，若 $s_n = 0$，由于 $R' = R/\mathfrak{q}_{i+1}$ 是整环，故 r 适合一个次数更低的首一多项式

$$g(x) = x^{n-1} + s_1 x^{n-2} + \cdots + s_{n-1}.$$

于是立得

$$S' \ni s_n = -r^n - s_1 r^{n-1} - \cdots - s_{n-1} r \in \mathfrak{q}'_i,$$

即 $0 \neq s_n \in S' \cap \mathfrak{q}'_i = \mathfrak{p}'_i$。 ▌

与定理6.8（诺德正规化定理）结合，我们证明下面的两个定理。

定理6.24 $\dim K[x_1, \cdots, x_n] = n$，此处$K$是域，$x_1, \cdots, x_n$是变数。

证明 应用数学归纳法。如果 $n = 0$，显然 $\dim K = 0$。设已知

$$\dim[x_1, \cdots, x_{n-1}] = n - 1.$$

在 $K[x_1,\cdots,x_n]$中任取一素理想链

$$(*)\qquad \mathfrak{q}_0 \supsetneqq \mathfrak{q}_1 \supsetneqq \cdots \supsetneqq \mathfrak{q}_m \supsetneqq (0)。$$

取 $f\in \mathfrak{q}_m, f\neq 0$。令 $f=\Pi f_i$ 为 f 的素元分解式。因为 $\mathfrak{q}_m$ 是素理想，所以必有一不可分解的多项式 $f_i\in \mathfrak{q}_m$。即令 f 为一不可分解的多项式。应用变数代换：

$$z_n=x_n,\quad z_{n-1}=x_{n-1}-x_n^{l_{n-1}},\quad \cdots,\quad z_1=x_1-x_n^{l_1},$$

其中 $0\ll l_{n-1}\ll\cdots\ll l_2\ll l_1$。令 f 为下面的形式

$$f=a_0 z_n^l+a_1(z_1,\cdots,z_{n-1})z_n^{l-1}+\cdots+a_l(z_1,\cdots,z_{n-1}),$$

其中 $a_0\neq 0$。不难看出，$K[x_1,\cdots,x_n]=K[z_1,\cdots,z_n]$。令

$$R=K[z_1,\cdots,z_n]/(f),$$

$$S=K[z_1,\cdots,z_{n-1}],\qquad \mathfrak{q}_i'=\mathfrak{q}_i/(f)。$$

则有：1）z_n 是对 S 整数相关的，因此 R 是对 S 整数相关的，$R\supset S$。所以 $\dim R=\dim S$。2）根据归纳法的假设，$\dim S=n-1$。3）下面是 R 的一个素理想链

$$\mathfrak{q}_0'\supsetneqq \mathfrak{q}_1'\supsetneqq\cdots\supsetneqq \mathfrak{q}_m'。$$

综合以上的三点，立得$m\leqslant n-1$。考虑(*)式，不难推出

$$\dim K[x_1,\cdots,x_n]\leqslant n。$$

又显然

$$(x_1,\cdots,x_n)\supsetneqq(x_1,\cdots,x_{n-1})\supsetneqq\cdots\supsetneqq(x_1)\supsetneqq(0)$$

是 $K[x_1,\cdots,x_n]$ 的一个素理想链，所以

$$\dim K[x_1,\cdots,x_n]=n。\quad \blacksquare$$

定理6.25 设 $R=K[r_1,\cdots,r_m]$ 是整环，此处 K 是域。令 F 为 R 的比域，则恒有

$$\dim R=\operatorname{tr\,deg} F/K,$$

即 R 的维数等于 F 对 K 的超越次数。

证明 应用定理6.8，存在 $S=K[x_1,\cdots,x_n]\subset R$，$R$ 对 $K[x_1,\cdots,x_n]$ 是整数相关的，$x_1,\cdots,x_n$ 是变数。根据上面两个定理，有 $\dim R=\dim S=n$。不难看出，F 是 $K(x_1,\cdots,x_n)$ 的代数扩域，所以

$$\operatorname{tr}\deg F/K=\operatorname{tr}\deg K(x_1,\cdots,x_n)/K=n. \quad \blacksquare$$

讨论 超越次数 $\operatorname{tr}\deg F/K$ 可以当成空间的自由度的代数定义。例如，定义在 n 维仿射空间上的有理函数集，即 $K(x_1,\cdots,x_n)$，其超越次数也是 n，等同于空间的自由度。上面的定理说明了，本节开始时讨论的维数的定义 1）及 3）在同时有意义时是相同的。▎

以下，我们要用局部化来讨论维数。

定理6.26 设 S 是环。我们恒有

$$\dim S=\sup\{\dim S_{\mathfrak m}: \mathfrak m \text{ 是极大理想}\}.$$

证明 任取 S 的素理想链如下，其中 $\mathfrak m$ 是极大理想：

$$\mathfrak m\supsetneqq\mathfrak p_1\supsetneqq\mathfrak p_2\supsetneqq\cdots\supsetneqq\mathfrak p_n. \tag{1}$$

则有

$$\mathfrak m S_{\mathfrak m}\supsetneqq\mathfrak p_1S_{\mathfrak m}\supsetneqq\mathfrak p_2S_{\mathfrak m}\supsetneqq\cdots\supsetneqq\mathfrak p_nS_{\mathfrak m}. \tag{2}$$

所以

$$\dim S\leqslant\sup\{\dim S_{\mathfrak m}: \mathfrak m \text{ 是极大理想}\}.$$

反之，设有 $S_{\mathfrak m}$ 的素理想链如下：

$$\mathfrak m S_{\mathfrak m}\supsetneqq\mathfrak q_1\supsetneqq\mathfrak q_2\supsetneqq\cdots\supsetneqq\mathfrak q_n,$$

则令 $\mathfrak p_i=\mathfrak q_i\cap S$，立得(1)式。于是

$$\dim S\geqslant\sup\{\dim S_{\mathfrak m}: \mathfrak m \text{ 是极大理想}\}. \quad \blacksquare$$

讨论 这个定理是说，在几何的情形，一个代数多样体的维数等于各几何点（相当于极大理想）邻域的维数的极大值。这是很合于几何直观的。▎

我们可以把以上的维数论的讨论，推广到一般的理想。现给出下面的定义。

定义6.13 1）令 $\mathfrak p$ 是环 S 的素理想。定义 $\mathfrak p$ 的**高度**为

$$\operatorname{ht}(\mathfrak p)=\sup\{n: \text{存在一个素理想链 } \mathfrak p\supsetneqq\mathfrak p_1\supsetneqq\cdots\supsetneqq\mathfrak p_n\}.$$

如果 $\operatorname{ht}(\mathfrak p)=0$，则称 $\mathfrak p$ 为 S 的**极小素理想**。

2）令 I 是环 S 的任意理想，定义 I 的**高度**为

$$\operatorname{ht}(I)=\inf\{\operatorname{ht}(\mathfrak p): \mathfrak p\supset I\}.$$

讨论 1) 设$I=(x)\cap(x-1,y)\subset \boldsymbol{C}[x,y]$。则不难看出，

$$\mathrm{ht}(x)=1,\quad \mathrm{ht}(x-1,y)=2,\quad \mathrm{ht}(I)=1.$$

请注意，$\mathscr{V}(x)$是y轴，$\mathscr{V}(x-1,y)$是点$(1,0)$。$\mathscr{V}(I)$是y轴与点$(1,0)$的并集。因此，高度ht相当于**余维数**(即$\dim \boldsymbol{C}[x,y]-\dim\mathscr{V}(I)$)：

$$\mathrm{ht}(x)=1=2-\dim\mathscr{V}(x),$$
$$\mathrm{ht}(x-1,y)=2=2-\dim\mathscr{V}(x-1,y),$$
$$\mathrm{ht}(I)=1=2-\dim\mathscr{V}(I).$$

2) 不难看出，若$\mathfrak{p}$是素理想，则恒有$\mathrm{ht}(\mathfrak{p})=\dim S_{\mathfrak{p}}$。 ∎

为了便于后面的讨论，我们引入下面的有用的定义及引理。

定义6.14 设S是环，$S\neq 0$。S的Jacobson **根理想**定义为所有极大理想的交集，记为$\mathrm{rad}(S)$。

讨论 所有形如$1+a(a\in\mathrm{rad}(S))$的元素，不属于S的任何极大理想，因此必然是可逆元。反之，设I是一个理想，如果对于任意的$a\in I$，$1+a$都是可逆元，则必有$I\subset\mathrm{rad}(S)$。这是因为，假若$I\not\subset\mathrm{rad}(S)$，则必有某个$a\in I$，以及某个极大理想$\mathfrak{m}$，使$a\notin\mathfrak{m}$。令$\sigma: S\to S/\mathfrak{m}$为典型映射，则必存在$b\in S$，使$\sigma(ba)=-1$。不难看出，$ba\in I$，但$\sigma(1+ba)=0$，即$1+ba\in\mathfrak{m}$，也即$1+ba$不是可逆元，这与假设矛盾。

定理6.27(中山引理①) 设S是环，I是理想，M是S模，N及N'是M的子模。已知$M=N+IN'$，以及1) I是幂零的；或者2) $I\subset\mathrm{rad}(S)$以及N'是有限生成的。那么，我们恒有

$$M=N.$$

证明 1) $M/N=I(M/N)=I^2(M/N)=\cdots=0$。

2) 记$M'=M/N$，则$M'=IM'$。我们要证明$M'=0$。显然，M'是有限生成的S模。令

---

① 此引理即Nakayama引理(Nakayama的汉字写法是"中山正")。据永田雅宜研究，中山引理是Krull及東屋氏首先提出的，应称为"Krull-東屋引理"。因为中山引理已经广泛流传了，所以本书仍用旧名。

$$M' = \sum_{i=1}^{n} Sm_i.$$

我们用数学归纳法．如果 $n=1$，则有 $a \in I$，使$m_1 = am_1$，即$(1-a)m_1 = 0$。但 $a \in I \subset \text{rad}(S)$，故 $1-a$ 是可逆元，所以 $m_1 = 0$，也即 $M' = 0$。一般言之，我们要证明存在 $a' \in I$，使$(1+a')M' = 0$。令 $M'' = M'/Sm_n$。由归纳法假设，存在 $a \in I$，使 $(1+a)M'' = 0$，即 $(1+a)M' \subset Sm_n$。用 $M' = IM'$ 代入，即有

$$(1+a)M' = (1+a)IM' \subset ISm_n = Im_n.$$

于是存在 $b \in I$，使 $(1+a)m_n = bm_n$。不难看出，下式

$$(1+a)(1+a-b) = 1 + (2a - b + a^2 - ab) = 1 + a'$$

中的 a' 即所求。▎

我们要引入 S 模 M 的"长度"的概念。所谓 M 的一个**正规序列**，是指下面的一个子模链

$$M = M_0 \supset M_1 \supset M_2 \supset \cdots \supset M_r = 0.$$

r即称为这个正规序列的**长度**．如果$M_i \neq M_{i+1}$($\forall i = 0,1,\cdots,r-1$)，则称上面的正规序列是沒有重复的，如果上面的正规序列是沒有重复的，而且在 M_i 与M_{i+1}之间，沒有别的子模，则称之为一个**合成序列**.

一般言之，任给一个模，并不一定有合成序列。例如，在 $\mathbf{Z}$ 中，我们有 $(2) \supsetneqq (2^2) \supsetneqq (2^3) \supsetneqq \cdots$，这个子模链是永不终止的。又如，在 $\mathbf{C}[x]$中，我们有

$$(x) \supsetneqq (x^2) \supsetneqq (x^3) \supsetneqq \cdots.$$

但是我们有如下的定理。

定理6.28(Jordan 定理)　如果 S 模 M 中有一个长度为 r 的合成序列，那么每一个合成序列的长度都是 r，并且每一个沒有重复的正规序列都可以加细成一个合成序列。

证明　读者仿照群论的若当-荷德定理，自行证明。▎

定义6.15　设 S 模 M 有一个合成序列，则我们定义模 M 的**长度**即为此合成序列的长度，记为 $\text{length}_S M$。按照上面的定理，

这是所有合成序列的共同的长度。如果 M 没有合成序列，则定义 $\text{length}_S M=\infty$。

我们从维数论的角度，研究最简单的环 S，即 $\dim S=0$ 的情形。设 S 是域，则自然有 $\dim S=0$。反之，$\dim S=0$ 定义了什么样的环 S 呢？事实上，S 必为 Artin 环。这是我们要在本节说明的。我们先给出下面的定义。

定义6.16 如果 S 的理想的任一下降的链必然终止，则称 S 为 Artin 环。即设有下面的链

$$I_1\supset I_2\supset\cdots\supset I_n\supset I_{n+1}\supset\cdots,$$

其中 I_n 皆是 S 的理想。则必存在一 m，使

$$I_m=I_{m+1}=\cdots.$$

定理6.29 1) S 是 Artin 环 $\Longleftrightarrow \text{length}_S S<\infty$；

2) S 是 Artin 环 $\Longleftrightarrow S$ 是诺德环，且 $\dim S=0$。

证明 1) $\Longleftarrow$。此时，S 当作 S 模，它的子模即是环 S 的理想，因此，S 必然是 Artin 环。

$\Longrightarrow$。我们先证明 S 只有有限多个极大理想。否则，设 $\mathfrak{m}_1,\mathfrak{m}_2,\cdots,\mathfrak{m}_n,\cdots$ 是 S 的无限多个互不相同的极大理想，考虑下面的理想链

$$\mathfrak{m}_1\supset\mathfrak{m}_1\mathfrak{m}_2\supset\cdots\supset\mathfrak{m}_1\mathfrak{m}_2\cdots\mathfrak{m}_n\supset\cdots.$$

我们只要证明相邻的两个理想都不相等便足够了。假设

$$\mathfrak{m}_1\mathfrak{m}_2\cdots\mathfrak{m}_{n-1}=\mathfrak{m}_1\mathfrak{m}_2\cdots\mathfrak{m}_{n-1}\mathfrak{m}_n\subset\mathfrak{m}_n.$$

不难看出，必有某个 $i<n$，使 $\mathfrak{m}_i\subset\mathfrak{m}_n$。于是 $\mathfrak{m}_i=\mathfrak{m}_n$。这与 $\mathfrak{m}_1,\mathfrak{m}_2,\cdots$ 互不相同矛盾。

现设 $\mathfrak{m}_1,\mathfrak{m}_2,\cdots,\mathfrak{m}_r$ 是 S 的所有的极大理想。令

$$I=\mathfrak{m}_1\mathfrak{m}_2\cdots\mathfrak{m}_r.$$

考虑下面的下降的理想链：

$$I\supset I^2\supset I^3\supset\cdots.$$

由于 S 是 Artin 环，所以必有一 m 存在，使

$$I^m=I^{m+1}=\cdots,$$

令 $$J=(0):I^m=\{a:\ aI^m=(0)\}.$$
我们要证明 $J=S$。如此，则 $I^m=(0)$。

假若 $J\neq S$。令 J' 为包含 J 而且不等于 J 的理想中的极小者。为什么存在这样一个 J' 呢？请参考定理3.25。在那里我们证明了诺德环与极大原则是等同的。同样的道理，可以证明 Artin 环与“极小原则”是等同的(读者试自证之)。因此有这样的J'存在。任取 $a\in J'\setminus J$，则 $J'=J+(a)$。显然，$I\subset\mathrm{rad}(S)$，根据定理6.27(Nakayama 引理)，则知$J+aI\neq J'$。再根据 J' 的选取，立得 $J+aI=J$。于是 $aI\subset J$，即有
$$a\in J:I=((0):I^m):I=(0):I^{m+1}=0:I^m=J.$$
这与 a 的选取是矛盾的。因此 $J=S$，$I^m=(0)$。

以下，我们考虑一个理想链：
$$S\supset\mathfrak{m}_1\supset\mathfrak{m}_1\mathfrak{m}_2\supset\cdots\supset\mathfrak{m}_1\mathfrak{m}_2\cdots\mathfrak{m}_r\supset I\mathfrak{m}_1\supset\cdots$$
$$\supset I^2\supset I^2\mathfrak{m}_1\supset\cdots\supset I^m=(0).$$
相邻两项的商模是域 $S/\mathfrak{m}_i$ 上的向量空间，此向量空间的子空间对应到这两项间的理想。根据 Artin 环的条件，知这些商模都是有限维向量空间，于是它们都是有限长度的 S 模，而 $\mathrm{length}_S S$ 即是这些长度的和，于是 $\mathrm{length}_S S<\infty$。

2) $\Longrightarrow$。根据 1)，S 显然是诺德环。我们用上面的符号。任取 $\mathfrak{p}\in\mathrm{Spec}(S)$，则有
$$(\mathfrak{m}_1\mathfrak{m}_2\cdots\mathfrak{m}_r)^m=(0)\subset\mathfrak{p},$$
所以必有某个 i，使 $\mathfrak{p}=\mathfrak{m}_i$。也即所有素理想都是极大理想。立得 $\dim S=0$。

$\Longleftarrow$。令$(0)=\bigcap\limits_{i=1}^{r}I_i$ 是理想(0)的简略准素分解，$\mathfrak{p}_i=\sqrt{I_i}$。因为 $\mathfrak{p}_i$ 是有限生成的，不难看出，存在正整数 m_i，使 $\mathfrak{p}_i^{m_i}\subset I_i$。令 $m=\max\{m_1,\cdots,m_r\}$，则有
$$(\mathfrak{p}_1\cdots\mathfrak{p}_r)^m\subset\bigcap_{i=1}^{r}I_i=(0),$$

所以$(\mathfrak{p}_1\cdots\mathfrak{p}_r)^n=\bar{0}$。自然，因为$\dim\bar{S}=0$，所以诸$\mathfrak{p}_i$都是极大理想。令$I=\mathfrak{p}_1\cdots\mathfrak{p}_r$，我们应用1)的证明中的最后一段，立即得$\text{length}_S S<\infty$。因此，$S$是Artin环。∎

系 设诺德环的有限多个极大理想$\mathfrak{m}_1,\cdots,\mathfrak{m}_n$的乘积(或交集)是(0)，则$S$是Artin环。

证明 我们只要证明$\dim S=0$就足够了。换句话说，我们要证明S的任意素理想$\mathfrak{p}$都是极大理想。自然，我们有

$$\mathfrak{p}\supset(0)=\mathfrak{m}_1\cdots\mathfrak{m}_n \text{ 或 } \mathfrak{p}\supset(0)=\bigcap_{i=1}^{n}\mathfrak{m}_i.$$

所以$\mathfrak{p}$等于某个$\mathfrak{m}_i$。∎

例15 令

$$A=\boldsymbol{C}[x,y]_{(x,y)},\qquad S_1=A/(x,y),$$
$$S_2=A/(x,x+y^2),\qquad S_3=A/(x+y^4,x+y^3),$$

S_1,S_2,S_3都是Artin环。经过计算得

$$\dim_C S_i=\text{length}_S S_i=i.$$

这正好是S_i对应的那两条曲线在原点相交的次数。∎

在第八章“Dedekind整环”中，我们将讨论$\dim S\leqslant 1$的情形。在那里，我们将统一讨论“代数曲线论”及“代数数论”。

习　题

1. 令$R=\boldsymbol{C}[x_1,x_2,\cdots,x_n]/(f(x_1,x_2,\cdots,x_n))$，这里$f(x_1,x_2,\cdots,x_n)$是一个不可约的多项式。证明$\dim R=n-1$。

2. 考察$\mathscr{V}((xz,yz))\subset\boldsymbol{A}^3$在各点的维数，即令

$$R=\boldsymbol{C}[x,y,z,]/(xy,yz),$$

考察$\dim R_{\mathfrak{m}}$($\forall R$的极大理想$\mathfrak{m}$)。

3. 参考上题，求出$\text{ht}(xz,yz)$。

4. 令R是一个局部环，$\mathfrak{m}$是它的极大理想。设$x_1,x_2,\cdots,x_n\in R$。如果

$$(x_1,x_2,\cdots,x_n)+\mathfrak{m}^2=\mathfrak{m},$$

证明$(x_1,x_2,\cdots,x_n)=\mathfrak{m}$。

5. 令$R=\mathbf{C}[x,y]_{(x,y)}$。证明$R$中的理想的等式：

$$(x+x^{10}y,y+x^3y^5)=(x,y).$$

6. 设R是局部环，$\mathfrak{m}$为其极大理想，M是有限R模，则$M/\mathfrak{m}M$是域$R/\mathfrak{m}$上的有限维向量空间。设其基为$\bar{x}_1,\bar{x}_2,\cdots,\bar{x}_n$。取$\bar{x}_i$在$M$中的原象$x_i$(即$\bar{x}_i=x_i+\mathfrak{m}M$)，由Nakayama引理知$x_1,x_2,\cdots,x_n$是$M$的$R$模生成元。试举一例，说明$x_1,x_2,\cdots,x_n$可以$R$线性相关。

7. 设K为域。再设有有限维K向量空间的正合序列

$$0\xrightarrow{f_0}M_1\xrightarrow{f_1}M_2\xrightarrow{f_2}\cdots\longrightarrow M_{n-1}\xrightarrow{f_{n-1}}M_n\xrightarrow{f_n}0,$$

(即f_i为K线性映射，$\ker f_i=\operatorname{im}f_{i-1}$，$\forall i=1,2,\cdots,n$)。证明

$$\operatorname{length}_K M_i=\dim_K M_i$$

且

$$\sum_{i=1}^{n}(-1)^i\operatorname{length}_K M_i=0.$$

8. 证明Artin整环是域。

9. 设R是主理想整环，$\mathfrak{a}$是R的非零理想。证明$R/\mathfrak{a}$是Artin环。

10. 设R是诺德环。证明R是Artin环$\Longleftrightarrow\operatorname{Spec}R$是离散的。

11. 设k是域，$R=k[x_1,x_2,\cdots,x_n]$（x_i不一定代数无关)。证明R是Artin环$\Longleftrightarrow R$作为k模是有限的。

12. 只有一个素理想的局部环称为**准素环**(primary ring)。证明每一个诺德准素环必是Artin环。

13. 证明每一个Artin环是有限多个诺德准素环的直和，而这样的直和分解是唯一的。

14. 构造一个无限维诺德整环。

§7 分次环及分次模

我们考虑常见的多元多项式环$K[x_1,\cdots,x_n]=S$。我们可以

自然地把S当作n维仿射空间K^n上面的多项式函数的集合。当我们在K^n里取坐标系$(x_1,\cdots,x_n)$时，S就自然写成了$K[x_1,\cdots,x_n]$。我们取不同的坐标系$(y_1,\cdots,y_n)$时，S当然就是$K[y_1,\cdots,y_n]$了。一般说来，$(x_1,\cdots,x_n)$与$(y_1,\cdots,y_n)$两个坐标系之间的关系不一定是线性的。例如

$$y_1=x_1,\quad y_2=x_2+x_1^2,\quad \cdots,\quad y_n=x_n+x_1^n.$$

此时，$f\in S$对两个坐标系可能有不同的次数。例如，y_i对坐标系$(y_1,\cdots,y_n)$是一次式，可是对坐标系$(x_1,\cdots,x_n)$却是i次式了。

但是，如果我们不是考虑仿射空间K^n，而是考虑射影空间

$$P^n=\{K^{n+1}\text{ 中通过原点的直线}\},$$

那么K^{n+1}的两个坐标系$(x_0,x_1,\cdots,x_n)$与$(y_0,y_1,\cdots,y_n)$之间只允许线性变换的差异了。如果令$R=K[x_0,x_1,\cdots,x_n]$，则$f\in R$的次数是不随坐标变换而改变的。在这种情况下，R自然地写成

$$R=\bigoplus_{i\geqslant 0}R_i,\qquad R_i=i\text{ 次齐次多项式的集合。}$$

定义6.17 1）设环$R=\bigoplus_{i\geqslant 0}R_i$，此处$R_i$是加法子群。如果

$$R_iR_j\subset R_{i+j},\qquad \forall\ i,j\geqslant 0,$$

则称R是一个**分次环**，R_i的非零元素称为i次齐次元。对于$r_i\in R_i$，$r_i\neq 0$，定义其次数为$\deg r_i=i$；

2）设$R=\bigoplus_{i\geqslant 0}R_i$是分次环，$M$是$R$模。如果$M=\bigoplus_{i\geqslant 0}M_i$，此处$M_i$是子群，适合

$$R_iM_j\subset M_{i+j},$$

则称M是**分次模**；M_i的非零元素称为i次齐次元。如果$m_i\in M_i$，$m_i\neq 0$，则$\deg m_i=i$。

讨论 因为$R_0R_0\subset R_0$，所以R_0对乘法是封闭的。又因为$1\cdot R_i\subset R_i$，所以$1\in R_0$。不难推导出R_0是一环。令

$$R_+=\sum_{i>0}R_i,$$

容易看出 R_+ 是 R 的理想。

例16 设 $S=\mathbf{C}[x^2,x^3]$，$I=(x^2,x^3)$。令 $R_0=S/I=\mathbf{C}$，$R_1=I/I^2,\cdots,R_n=I^n/I^{n+1},\cdots$。一般说来，

$$I^n=(x^{2n},x^{2n+1},x^{2n+2},\cdots)=(x^{2n},x^{2n+1})。$$

记 $I^n/I^{n+1}=\mathbf{C}y^{2n}+\mathbf{C}y^{2n+1}$，则

$$R=\bigoplus_{i\geq 0}R_i=\mathbf{C}\oplus[\mathbf{C}y^2\oplus\mathbf{C}y^3]\oplus\cdots\oplus[\mathbf{C}y^{2n}\oplus\mathbf{C}y^{2n+1}]\oplus\cdots$$

是一分次环。▎

通常说来，任取环 S，理想 I 及 S 模 M，则$\{I^i\}$ $(I^0=S)$是下降的理想链，$\{I^iM\}$是下降的子模链。我们定义

$$G_I(S)=\bigoplus_{i=0}^{\infty}I^i/I^{i+1},\quad G_I(M)=\bigoplus_{i=0}^{\infty}I^iM/I^{i+1}M。$$

自然 I^i/I^{i+1} 及 $I^iM/I^{i+1}M$ 都是加法交换群。我们认定它们的元素是 i 次齐式元。

我们定义 $G_I(S)$与$G_I(M)$的乘法如下：设

$$\bar{a}\in I^i/I^{i+1},\quad \bar{m}\in I^jM/I^{j+1}M,$$

此处 $a\in I^i$，$m\in I^jM$。定义

$$\bar{a}\cdot\bar{m}=\overline{am}\in I^{i+j}M/I^{i+j+1}M。$$

显然这个定义是良好的。我们再定义

$$\left(\sum_i\bar{a}_i\right)\cdot\left(\sum_j\bar{m}_j\right)=\sum_{i,j}\bar{a}_i\bar{m}_j。$$

不难看出，这样定义的乘法，当 $M=S$ 时，使得 $G_I(S)$成为一环；当 M 为任意 S 模时，使得 $G_I(M)$为$G_I(S)$模。我们称 $G_I(S)$为**与理想 I 相伴的分次环**，$G_I(M)$为**与理想 I 相伴的分次模**。

例17 令 $S=\mathbf{C}[x,y]_{(x,y)}$，$I=(x,y)$。不难看出，

$$I^i=(x^i,x^{i-1}y,\cdots,y^i),$$

$$I^i/I^{i+1}=\mathbf{C}\bar{x}^i\oplus\mathbf{C}\bar{x}^{i-1}\bar{y}\oplus\cdots\oplus\mathbf{C}\bar{y}^i,$$

于是

$$G_I(S)=\mathbf{C}[\bar{x},\bar{y}]\approx\mathbf{C}[x,y]。$$

定理6.30 1) 设 R 是分次环。则 R 是诺德环 $\Longleftrightarrow R_0$ 是诺德环，以及 $R=R_0[r_1,\cdots,r_s]$；

2) 设 R 是诺德分次环，M 是有限生成的分次 R 模。那么，每一个 M_i 都是有限生成的 R_0 模。

证明 1) $\Longleftarrow$。显然。

$\Longrightarrow$。$R_0\approx R/R_+$，所以 R_0 是诺德环。R_+ 是有限生成的理想。取它的生成元集 $\{f_1,\cdots,f_n\}$。设

$$f_i=\sum_j g_{ij}\quad,$$

其中 g_{ij} 是 j 次齐次元。则显然，$\{g_{ij}\}$ 也是 R_+ 的生成元。所以可以取 R_+ 的一个齐次生成元集 $\{r_1,\cdots,r_s\}$。现在要证明 $R=R_0[r_1,\cdots,r_s]$。任取 R_+ 的齐次元 f，设

$$f=\sum_i g_i r_i.$$

显然可以弃去所有 $\deg g_i+\deg r_i\neq\deg f$ 的项。所以可设

$$\deg g_i=\deg f-\deg r_i<\deg f.$$

用数学归纳法，立得 $g_i\in R_0[r_1,\cdots,r_s]$。所以 $f\in R_0[r_1,\cdots,r_s]$。即 $R=R_0[r_1,\cdots,r_s]$。

2) 我们可以同上面类似地选取 M 的一个齐次生成元集 $\{m_1,\cdots,m_t\}$ 以及 R 的一个齐次生成元集 $\{r_1,\cdots,r_s\}$。则有

$$R=R_0[r_1,\cdots,r_s].$$

显然，M_i 作为 R_0 模是由 $\{y_j m_j: y_j$ 是 $r_1,\cdots,r_s$ 的单项式，$\deg y_j+\deg m_j=i\}$ 生成的，这显然是有限集。▍

我们考虑 R 是诺德分次环、R_0 是 Artin 环、M 是有限生成的分次 R 模的情形。按照定理6.30，每一个 M_i 都是有限生成的 R_0 模，因此都有一个合成序列(请读者想想，为什么？)，所以

$$\text{length}_{R_0}M_i<\infty.$$

令 $l(M_i)=\text{length}_{R_0}M_i$，则下面的级数称为 M 的Poincaré 级数：

$$P(M,t)=\sum_{i=0}^{\infty}l(M_i)t^i.$$

我们先用几个例子来说明 Poincaré 级数的意义，然后再从事一般理论性的探讨。

例18 令 $M = S = K[x_1, \cdots, x_n] = \bigoplus\limits_{i \geq 0} S_i$，其中 S_0 为域 K，S_i 为 i 次齐次多项式的集合。经过简单计算，得出

$$l(S_i) = \binom{n+i-1}{i} = \binom{n+i-1}{n-1},$$

故

$$P(S,t) = \sum_{i=0}^{\infty} \binom{n+i-1}{n-1} t^i.$$

我们要说明 $P(S,t) = 1/(1-t)^n$。

证法一。直接展开：

$$\begin{aligned}\frac{1}{(1-t)^n} &= 1 + \sum_{i=1}^{\infty} \binom{-n}{i} (-1)^i t^i \\ &= 1 + \sum_{i=1}^{\infty} \frac{(-n)(-n-1)\cdots(-n-i+1)}{i!} (-1)^i t^i \\ &= 1 + \sum_{i=1}^{\infty} \binom{n-1+i}{i} t^i\end{aligned}$$

证法二。当 $n=1$ 时，

$$P(S,t) = 1 + t + \cdots + t^i + \cdots = \frac{1}{1-t}.$$

用归纳法。令 $S' = K[x_1, \cdots, x_{n-1}] = \bigoplus S'_i$，$S'' = K[x_n] = \bigoplus S''_i$。则显然有

$$l(S_i) = \sum_{p+q=i} l(S'_p) l(S''_q).$$

代入，立得

$$P(S,t) = P(S',t)P(S'',t) = \frac{1}{(1-t)^{n-1}} \frac{1}{(1-t)} = \frac{1}{(1-t)^n}.$$

另外一个有趣的计算，是把 $l(S_i)$ 写成 i 的多项式 $\chi(i)$。令

$$\binom{x}{m}=\frac{x(x-1)\cdots(x-m+1)}{m!}.$$

不难看出

$$\begin{aligned}\binom{i+n-1}{n-1}&=\binom{i+n-2}{n-1}+\binom{i+n-2}{n-2}\\&=\binom{i+n-3}{n-1}+2\binom{i+n-3}{n-2}+\binom{i+n-3}{n-3}\\&=\cdots\cdots\\&=\binom{i}{n-1}+\binom{n-1}{1}\binom{i}{n-2}+\cdots\\&\quad+\binom{n-1}{n-2}\binom{i}{1}+1,\end{aligned}$$

即有

$$(*)\qquad \chi(x)=\binom{x}{n-1}+\binom{n-1}{1}\binom{x}{n-2}+\cdots+\binom{n-1}{n-2}\binom{x}{1}+1.$$

以后，我们将称 $\chi(x)$ 为 Hilbert 多项式。请注意，$K[x_1,\cdots,x_n]$ 对应于 $n-1$ 维射影空间 $\boldsymbol{P}^{n-1}$，此时 $\deg\chi(x)=n-1=\dim\boldsymbol{P}^{n-1}$。$\boldsymbol{P}^{n-1}$ 一般看成一次代数多样体，而(*)式的首项系数正好是1。又有 $\boldsymbol{P}^{n-1}$的"算术亏格"是 0，将(*)式的常数项 $a_{n-1}(=1)$ 代入 $(-1)^{n-1}(a_{n-1}-1)$后，此式正好等于 0。这些都不是偶然的巧合。一般我们用 $(-1)^{n-1}(a_{n-1}-1)$ 来定义所谓**算术亏格**。

例19 仿照上面的例子，计算

$$R=\boldsymbol{C}[x_1,x_2,x_3]/(f(x_1,x_2,x_3)).$$

此处 $f(x_1,x_2,x_3)$ 是一个 m 次齐次式。自然，$f(x_1,x_2,x_3)=0$ 定义了射影平面 $\boldsymbol{P}^2$ 上的一条代数曲线。

令 $S = \boldsymbol{C}[x_1, x_2, x_3] = \bigoplus_{i \geq 0} S_i$，其中 S_i 为 i 次齐次式的集合。令 $R = \bigoplus_{i \geq 0} R_i$，则当 $i \geqslant m$ 时，有 $R_i = S_i / fS_{i-m}$。所以

$$l(R_i) = l(S_i) - l(S_{i-m}) = \binom{i+2}{2} - \binom{i-m+2}{2}$$

$$= m\binom{i}{1} + \left(1 - \frac{(m-1)(m-2)}{2!}\right)$$

$$= a_0\binom{i}{1} + a_1,$$

其中 $a_0 = m, a_1 = 1 - (m-1)(m-2)/2$。此时，Hilbert 特征多项式为(详见后文)

$$\chi(x) = m\binom{x}{1} + \left(1 - \frac{(m-1)(m-2)}{2}\right).$$

当 $i \geqslant m$ 时，$\chi(i) = l(R_i)$。$\chi(x)$的次数 1 等于 $f(x_1, x_2, x_3) = 0$ 所定义的代数曲线的复维数，它的首项系数 m 等于代数曲线的重数(multiplicity)。$(-1)^1(a_1 - 1) = (m-1)(m-2)/2$ 等于代数曲线的算术亏格。当代数曲线无奇异点时，它的算术亏格等于几何亏格。例如，

$$f(x_1, x_2, x_3) = x_1^3 + x_2^3 - x_3^3,$$

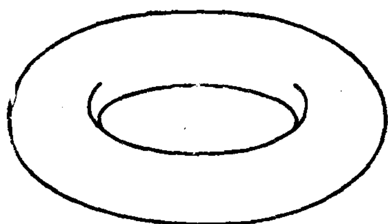


图 6.1

其相应的代数多样体的亏格是 1，直观上形如图 6.1 所示的中间有一洞的轮胎。请注意，这个代数多样体的实维数是 2，但是它的复维数是 1。

现在我们来计算R的 Poincaré 级数 $P(R,t)$：

$$P(R,t) = 1 + \binom{3}{2}t + \cdots + \binom{m+1}{2}t^{m-1} + \left[\binom{m+2}{2} - \binom{2}{2}\right]t^m +$$

$$+\cdots+\left[\binom{i+2}{2}-\binom{i-m+2}{2}\right]t^i+\cdots$$

$$=\frac{1}{(1-t)^2}-t^m\frac{1}{(1-t)^2}=\frac{1-t^m}{(1-t)^2}. \quad \blacksquare$$

为了得到 Poincaré 级数和 Hilbet 特征多项式的一般性质，我们先证明下面的引理。

引理 设 R_0 是 Artin 环，M_i 是有限生成的 R_0 模，设下面的序列是“正合”的：

$$0\xrightarrow{\sigma_0}M_0\xrightarrow{\sigma_1}M_1\xrightarrow{\sigma_2}\cdots\xrightarrow{\sigma_s}M_s\xrightarrow{\sigma_{s+1}}0.$$

这就是说，每个 σ_i 都是模映射，而且 $\mathrm{im}\,\sigma_i=\ker\sigma_{i+1}$ $(i=0,1,\cdots,s)$。那么，我们恒有

$$\sum_{i=0}^{s}(-1)^i l(M_i)=0.$$

证明 我们有下面的短正合序列

$$0\longrightarrow\mathrm{im}\,\sigma_i\longrightarrow M_i\longrightarrow\mathrm{im}\,\sigma_{i+1}\longrightarrow 0.$$

显然，$M_i/\mathrm{im}\,\sigma_i\approx\mathrm{im}\,\sigma_{i+1}$。不难得出

$$l(M_i)=l(\mathrm{im}\sigma_i)+l(\mathrm{im}\,\sigma_{i+1}).$$

所以

$$\sum_{i=0}^{s}(-1)^i l(M_i)=0. \quad \blacksquare$$

现在我们要证明下面的定理。请参看上面的两个例子。

定理6.31(Hilbert-Serre 定理) 设 R 是诺德分次环，R_0 是 Artin 环，$R=R_0[r_1,\cdots,r_n]$，r_i 均为齐次元，$\deg r_i=e_i>0$。又设 M 是一有限生成的分次 R 模。则存在一个多项式 $f(t)\in \mathbf{Z}[t]$，使

$$P(M,t)=\frac{f(t)}{\prod(1-t^{e_i})}.$$

证明 对生成集$\{r_1,\cdots,r_n\}$的基数n作归纳法。设$n=0$，$R=R_0$。那么，当m大于M的所有生成元的次数时，$M_m=0$，$l(M_m)=0$。于是$P(M,t)=f(t)\in \mathbf{Z}[t]$。

设已证$n-1$的情形。考虑下面的映射：

$$r_n^*: M\to M,$$
$$r_n^*(m)=r_n m.$$

自然，$r_n^*(M_i)\subset M_{i+e_n}$。令

$$K=\ker r_n^*=\oplus K_i,\qquad C=M/\operatorname{im} r_n^*=\oplus C_i,$$

于是我们有下面的正合序列

$$0\longrightarrow K_i\xrightarrow{j} M_i\xrightarrow{r_n^*} M_{i+e_n}\xrightarrow{\tau} C_{i+e_n}\longrightarrow 0,$$

其中j是嵌入映射，$\tau: M_{i+e_n}\to C_{i+e_n}=M_{i+e_n}/r_n^*(M_i)$是典型映射。不难看出，上面的序列确实是正合的。根据上面的引理，我们得到

$$l(K_i)-l(M_i)+l(M_{i+e_n})-l(C_{i+e_n})=0.$$

乘以t^{i+e_n}，令$i=0,1,2,\cdots$取和，得出

$$t^{e_n}P(K,t)-t^{e_n}P(M,t)+P(M,t)-P(C,t)+g(t)=0,$$

其中$g(t)$是一个多项式，它是由$P(M,t)$及$P(C,t)$缺少最初的e_n项而产生的。又知$r_nK=0$，$r_nC=0$，所以K,C都是R/r_nR模。而R/r_nR只须要次数为$e_1,\cdots,e_{n-1}$的$n-1$个生成元，用归纳法假设，立得

$$(1-t^{e_n})P(M,t)=P(C,t)-t^{e_n}P(K,t)-g(t)$$

$$=\frac{f(t)}{\prod\limits_{i=1}^{n-1}(1-t^{e_i})},$$

即有本定理。 ▎

我们又有下面的重要定理(请参看上面的两个例子)。

定理6.32(Hilbet-Serre 定理) 条件如定理6.31，更设$e_1=$

$e_2=\cdots=e_n=1$。那么，存在一个多项式 $\chi(x)\in Q[x]$，使得当 i 足够大时，$\chi(i)=l(M_i)$。这个 $\chi(x)$ 是唯一的，并且

$$\deg\chi(x)\leqslant n-1.$$

证明 用上面的定理，即知存在 $f(t)\in Z[t]$，使

$$P(M,t)=\frac{f(t)}{(1-t)^n}.$$

我们用部分分式展开上式的右侧，则得

$$P(M,t)=g(t)+d_0\frac{1}{(1-t)^n}+\cdots+d_{n-1}\frac{1}{1-t}.$$

参考例18，立得

$$P(M,t)=g(t)+\sum_{i=0}^{\infty}\left(\sum_{j=0}^{n-1}d_j\binom{i+n-j-1}{n-j-1}\right)t^i.$$

所以，当 $i>\deg g(t)$ 时，

$$l(M_i)=\sum_{j=0}^{n-1}d_j\binom{i+n-j-1}{n-j-1}.$$

即令
$$\chi(x)=\sum_{j=0}^{n-1}d_j\binom{x+n-j-1}{n-j-1},$$

其中
$$\binom{x}{s}=\frac{x(x-1)\cdots(x-s+1)}{s!}.$$

显然，$\chi(x)\in Q[x]$，$\deg\chi(x)\leqslant n-1$，当 $i\geqslant\deg g(t)$ 时，$\chi(i)=l(M_i)$。剩下的只须证唯一性了。设 $\chi^*(x)$ 是另外一个有同样性质的多项式，则 $\chi(x)-\chi^*(x)$ 对无限多个大的整数而言取值为零，因此必恒等于零，即 $\chi(x)=\chi^*(x)$。∎

讨论 不难看出，在上文取部分分式时，$d_0,d_1,\cdots,d_{n-1}$ 都是整数(因为 $f(t)\in Z[t]$)。我们通常不把

$$\chi(x)=\sum_{j=0}^{n-1}d_j\binom{x+n-j-1}{n-j-1}$$

展开成 x 的多项式，而是利用下面的恒等式

$$\binom{x+1}{s}=\binom{x}{s}+\binom{x}{s-1}$$

把 $\chi(x)$ 写成

$$\chi(x)=\sum_{j=0}^{n-1}d_j\binom{x+n-j-1}{n-j-1}=\sum_{j=0}^{n-1}a_j\binom{x}{n-j-1},$$

此时 $a_j\in Z\quad(j=0,1,\cdots,n-1)$。第一个非零的 a_j 必然是正整数（因为当 x 通过正整数趋于 ∞ 时，$\chi(x)>0$），称为 M 的次数(degree)或重数(multiplicity)或阶数(order)。在本章最后一节，我们将证明，在某些情形下，$d=\deg\chi(x)$ 相当于维数。又，$p_a=(-1)^d(a_{n-1}-1)$ 是"算术亏格"（参考例18及例19）。▌

我们现在回到 $G_I(S)$ 与 $G_I(M)$ 的讨论。设 $I=(a_1,\cdots,a_n)$ 为一个有限生成的理想．那么 $a_1,\cdots,a_n$ 的 i 次单项式的集合是 I^i 的一个生成元集．因此

$$G_I(S)=(S/I)[\bar{a}_1,\cdots,\bar{a}_n],$$

其中 $\bar{a}_i\in I/I^2$。所以，如果 S 是诺德环，或 S/I 是诺德环时，$G_I(S)$ 是诺德环。

如果 M 是有限生成的 S 模，$M=\sum_{j=1}^{m}Se_j$。那么 I^iM 是由 $a_1,\cdots,a_n$ 的 i 次单项式乘 e_j 生成的。不难看出 $G_I(M)$ 是由 $\{\bar{e}_1,\cdots,\bar{e}_m\}$ 生成的分次 $G_I(S)$ 模。自然，$\bar{e}_j\in M/IM$。

又设 I 包含有限多个极大理想的乘积或交集，那么，根据定理6.29的系，S/I 是 Artin 环。综上所述，在 S 是诺德环，M 是有限生成 S 模，I 包含有限多个极大理想的乘积或交集的情形下，$G_I(S)$ 和 $G_I(M)$ 适合定理6.31及定理6.32的要求。因此，我们可以定义 Poincaré 级数 $P(G_I(M),t)$ 以及 Hilbert 特征多项式 $\chi(x)$。特别是 S 是局部环，I 是它的极大理想，M 是有限生成 S 模时，我们可以如此考虑。

这样的考虑，有没有什么几何意义呢？我们回过头来研究例

17. 当 $S=\boldsymbol{C}[x,y]_{(x,y)}$，$I=(x,y)$时，

$$G_I(S)\cong \boldsymbol{C}[x,y]=\bigoplus G_i,$$

其中 G_i 为 i 次齐次式的集合. 因此

$$l(G_i)=i+1=\binom{i}{1}+1;$$

$$\chi(x)=\binom{x}{1}+1.$$

于是，$\deg\chi(x)=1\neq 2=\dim S$. 这不太恰当. 补救的办法，是取

$$l\left(\bigoplus_{j=0}^{i-1}G_j\right)=\sum_{j=0}^{i-1}(j+1)=\frac{i(i+1)}{2}=\binom{i}{2}+\binom{i}{1}.$$

令

$$\chi_I^S(x)=\binom{x}{2}+\binom{x}{1}.$$

则有 $\deg\chi_I^S(x)=2=\dim S$. 我们有下面的定理.

定理6.33 设 S 是诺德环，$I=(a_1,\cdots,a_n)$，S/I 是 Artin 环. 则存在唯一的多项式 $\chi_I^S(x)$，使得当 i 足够大时，

$$\chi_I^S(i)=l(S/I^i)=\sum_{j=0}^{i-1}l(I^j/I^{j+1}),$$

$\chi_I^S(x)$称为 S 对 I 的 Hilbert 特征多项式. $\deg\chi_I^S(x)\leqslant n$.

证明 用下面的恒等式:

$$\sum_{j=l}^{i-1}\binom{j}{l}=\binom{i}{l+1}.$$

按照定理6.32后面的讨论，当 j 足够大时，有

$$l(I^j/I^{j+1})=\sum_{l=0}^{n-1}a'_l\binom{j}{n-1-l}=\sum_{l=0}^{n-1}a_l\binom{j}{l},$$

其中 $a_l=a'_{n-1-l}$. 不难看出

$$l(S/I^i)=\sum_{j=0}^{i-1}\sum_{l=0}^{n-1}a_l\binom{j}{l}+\text{常数}=\sum_{l=0}^{n-1}\sum_{j=0}^{i-1}a_l\binom{j}{l}+\text{常数}$$

$$=\sum_{l=0}^{n-1}a_l\binom{i}{l+1}+\text{常数},$$

故

$$\chi_I^S(x)=\sum_{l=0}^{n-1}a_l\binom{x}{l+1}+\text{常数}. \quad \blacksquare$$

例20 设R是 Artin 环，$S=R[x_1,\cdots,x_n]$，$I=(x_1,\cdots,x_n)$。不难看出，$S=\oplus S_i$，其中S_i是i次齐次多项式的集合。易见

$$S/I^i\approx\{f(x_1,\cdots,x_n)\in S:\deg f<i\}.$$

因此

$$l(S/I^i)=\binom{i+n-1}{n}=\binom{i+n-2}{n}+\binom{i+n-2}{n-1}$$

$$=\binom{i}{n}+\sum_{j=1}^{n-1}\binom{n-1}{j}\binom{i}{n-j}.$$

于是

$$\chi_I^S(x)=\binom{x}{n}+\sum_{j=1}^{n-1}\binom{n-1}{j}\binom{x}{n-j},\qquad \deg\chi_I^S(x)=n.$$

习　题

1. 设R是分次环，S是R的乘法封闭子集。证明$S^{-1}R$也是分次环。

2. 设R是分次环，M是分次R模，N是M的子模。证明M/N是分次R模。

3. 设R是环，$\mathfrak{a}$是理想，并且$\bigcap_{n=1}^{\infty}\mathfrak{a}^n=\{0\}$。若$G_\mathfrak{a}(R)$是整环，证明$R$也是整环。

4. 设f是定义在$\boldsymbol{N}$上的整值函数(即$f(\boldsymbol{N})\subset\boldsymbol{Z}$)，这里$\boldsymbol{N}$

表示自然数集合。设又有 $g(x)\in \mathbf{Q}[x]$，$\deg g(x)=m-1$。如果

$$f(n+1)-f(n)=g(n),\quad \forall n\in \mathbf{N},$$

证明 $f\in \mathbf{Q}[x]$，且 $\deg f=m$。

5．设 I 为 $\mathbf{C}[x_1,\cdots,x_n]$ 中由 $x_1^2,\cdots,x_n^2$ 生成的理想，令

$$R=G_I(\mathbf{C}[x_1,\cdots,x_n]),$$

试计算 $P(R,t)$。又设 $S=\mathbf{C}[x_1,\cdots,x_n]/I$，$\mathfrak{m}$ 为 S 中由 $\bar{x}_1,\cdots,\bar{x}_n$ 生成的理想，试计算 $P(G_{\mathfrak{m}}(S),t)$。

6．设 $R=(\mathbf{C}[x,y]/(x^2-y^2-y^3))_{(\bar{x},\bar{y})}$，其中 $\bar{x},\bar{y}$ 为 x,y 在典范映射

$$\sigma:\ \mathbf{C}[x,y]\to \mathbf{C}[x,y]/(x^2-y^2-y^3)$$

下的象。令 $\mathfrak{m}=\bar{x}R+\bar{y}R$，求 $G_{\mathfrak{m}}(R)$，并考虑其几何意义。

7．令 $R=\mathbf{C}[x_1,x_2,x_3,x_4]/(x_2x_4-x_1^2,x_3x_4^2-x_1^3)$．计算 $P(R,t),\chi(x)$。试猜想其几何意义。

8．令 $R=\mathbf{C}[x,y,z,w]/(x^3-yzw,y^2-xz,z^2w-x^2y)$．计算 $P(R,t),\chi(x)$。

9．令 $R=\mathbf{C}[x,y]_{(x,y)}$，$f=x+$高次项，$S=R/(f),I=(\bar{x},\bar{y})$。计算 $\chi_I^S(x)$。

10．令 $R=\mathbf{C}[x,y]_{(x,y)}$，$f(x,y)=f_m(x,y)+$高次项，$f_m(x,y)$是$m$次齐次式。令 $S=R/(f),I=(\bar{x},\bar{y})$。计算 $\chi_I^S(x)$，试猜想其几何意义。

§8 拓 扑 环

在本章§4中，我们给出了环 S 的素谱集 Spec S 的 Zariski 拓扑，从而使 Spec S 成为一个拓扑空间。在本节中，我们将换一个题材，研究 S（而不是 Spec S）的各种拓扑。

一个环 S 中，给定一个拓扑，如果 S 的加法和乘法在这拓扑下都是连续的，则称 S 为一个**拓扑环**。又设 S 是拓扑环，M是 S 模，同时又是一个拓扑空间，而且M的模运算（即M的加法及 S

与M的乘法）都是连续的，则称M为一个**拓扑模**。

我们主要有兴趣的，是S由它的一个理想I的诸方幂

$$I \supset I^2 \supset \cdots \supset I^n \supset \cdots$$

所定义的如下的拓扑：

1）$I \supset I^2 \supset \cdots \supset I^n \supset \cdots$ 规定为0的邻域基，这就是说，S的子集L在0点是开的$\Longleftrightarrow$对某个n，$L \supset I^n$；

2）$a+I \supset a+I^2 \supset \cdots \supset a+I^n \supset \cdots$规定为$a$的邻域基。这就是说，$S$的子集在$a$点是开的$\Longleftrightarrow$对某个$n$，$L \supset a+I^n$；

3）S的子集是开集$\Longleftrightarrow$对任一$a \in L$，都有相应的n，使$L \supset a+I^n$。

不难看出，我们确实定义出S的一个拓扑。

定义6.18 以上所定义的拓扑，称S的I-adic拓扑。同样的，设M是S模。对$m \in M$，取

$$m+IM \supset m+I^2M \supset \cdots \supset m+I^nM \supset \cdots$$

为m的邻域基，则定义出M的一个拓扑，称为M的I-adic拓扑。

引理1 取M的I-adic拓扑。则M是Hausdorff空间(即对于任意两点$a, b \in M$，$a \neq b$，都有邻域$U_a \ni a, U_b \ni b$，使得$U_a \cap U_b = \varnothing$）$\Longleftrightarrow \bigcap\limits_{n=1}^{\infty} I^n M = \{0\}$。

证明 $\Longrightarrow$。假设$\bigcap\limits_{n=1}^{\infty} I^n M \neq \{0\}$，则存在$m \neq 0$，$m \in I^n M$ $(n=1,2,\cdots)$。考虑0的任一邻域U_0，必存在某个n，使得

$$U_0 \supset I^n M \ni m,$$

即$U_0 \cap U_m \neq \varnothing$，其中$U_m$为$m$的任一邻域，所以$M$不是Hausdorff空间。

$\Longleftarrow$。任取$m, m' \in M$，$m \neq m'$。则$m-m' \neq 0$，所以必有一n，使$I^n M \not\ni m-m'$。令

$$U_m = m+I^n M, \qquad U_{m'} = m'+I^n M.$$

假若有$m'' \in U_m \cap U_{m'}$，那么立得

$$m'' = m + am_1 = m' + bm_2, \quad a, b \in I^n, \ m_1, m_2 \in M.$$

即有
$$m - m' = bm_2 - am_1 \in I^n M,$$

这是不可能的。▍

引理 2 任取M的子集L，则L的闭包$\bar{L} = \bigcap_{n=1}^{\infty}(L + I^n M)$。

证明 设$m \in \bar{L}$。则m的每一个邻域$m + I^n M$都含有L的一个元素l_n，即$m + I^n M \ni l_n$，也即$m \in l_n + I^n M \subset L + I^n M$。立得

$$\bar{L} \subset \bigcap_{n=1}^{\infty}(L + I^n M).$$

反之，设$m \in \bigcap_{n=1}^{\infty}(L + I^n M)$，则有$m \in L + I^n M(\forall n = 1, 2, \cdots)$。即有$l_n \in L$，使$m \in l_n + I^n M$，$l_n \in m + I^n M$。所以$m \in \bar{L}$。▍

一个有趣的问题是：设N是M的子模，那么N可能有两个不同的I-adic拓扑。其一是把N看成S模(不是看作S的子模)，如此可得出N的一个I-adic拓扑；其二是先考虑M的I-adic拓扑，再由此拓扑在M的子集N上引生出一个拓扑。下面的定理将说明这两个拓扑是一致的。

定理6.34(Artin-Rees引理) 设S是诺德环，I是理想，M是有限生成的S模，N是M的子模。那么，必存在正整数r，使得当$n > r$时，我们恒有下式：

$$I^n M \cap N = I^{n-r}(I^r M \cap N).$$

说明 如果定理成立，我们就有

$$I^n N \subset I^n M \cap N \subset I^{n-r}(I^r M \cap N) \subset I^{n-r} N \subset I^{n-r} M \cap N,$$

所以$I^n M \cap N$与$I^n N(n = 1, 2, \cdots)$规定了N的同一个拓朴。

证明 令x是变数。考虑

$$S' = \bigoplus_{i=0}^{\infty} I^i x^i \subset S[x].$$

设$I = (a_1, \cdots, a_l)$，不难看出$S' = S[a_1 x, \cdots, a_l x]$。所以$S'$是诺德环。

同法，令

$$M' = \bigoplus_{i=0}^{\infty} I^i x^i M.$$

对于 $bx^i \in I^i x^i$，$cx^j m \in I^j x^j M$，定义

$$(bx^i)(cx^j m) = bcx^{i+j} m \in I^{i+j} x^{i+j} M,$$

立得 M' 是 S' 模。我们又令 $I^i x^i$ 及 $I^i x^i M$ 的元素为 i 次齐次元，则 S' 成为分次环，M' 成为分次 S' 模。当然，M 的生成元集也是 M' 的生成元集，所以 M' 也是有限生成的 S' 模。

令

$$N' = \left\{ \sum_{\text{有限}} z_i x^i : z_i \in I^i M \cap N \right\}.$$

显然 N' 是 M' 的一个子模，所以 N' 也是有限生成的 S' 模（为什么?）。令 $\{n_1 x^{e_1}, \cdots, n_q x^{e_q}\}$ 是 N' 的一个齐次生成元集，此处 $n_i \in I^{e_i} M \cap N$。令 $r = \max\{e_1, \cdots, e_q\}$。任取 $m \in I^n M \cap N$，此处 $n > r$。则 $mx^n \in N'$。所以

$$mx^n = \sum_{i=1}^{q} (a_i x^{n-e_i})(n_i x^{e_i}), \quad a_i \in I^{n-e_i}.$$

于是，我们得出

$$a_i n_i \in I^{n-r} I^{r-e_i} n_i \in I^{n-r}(I^r M \cap N).$$

但 $m = \sum a_i n_i$，所以 $I^n M \cap N \subset I^{n-r}(I^r M \cap N)$。反之，显然有

$$I^n M \cap N \supset I^{n-r}(I^r M \cap N). \ \blacksquare$$

定理6.35（交集定理） 设 S 是诺德环，I 是理想，M 是有限生成的 S 模。

1）令 $N = \bigcap_{i=1}^{\infty} I^i M$，则有 $IN = N$；

2）如果 $I \subset \text{rad}(S)$，则有 $\bigcap_{i=1}^{\infty} I^i M = \{0\}$。换句话说，$M$ 对 I-adic 拓扑是 Hausdorff 空间；

3）(Krull) 如果 $I = \text{rad}(S)$，则有 $\bigcap_{n=1}^{\infty} I^n = (0)$。特别是当

S为局部环，I是它的极大理想时，$\bigcap_{i=1}^{\infty} I^{n}=(0)$。

证明 1）当n足够大时，

$$N=\bigcap I^{n} M=I^{n} M \cap N=I(I^{n-1} M \cap N) \subset I N \subset N,$$

所以$IN=N$。

2）用中山引理，立得。

3）是2)的特例。 ▎

系(Krull) 设S是诺德整环，$I \subsetneqq S$为理想。那么

$$\bigcap_{n=1}^{\infty} I^{n}=(0).$$

证明 令$N=\bigcap_{n=1}^{\infty} I^{n}$，则有$IN=N$。仿照中山引理的证明，读者不难验证必有一$a \in I$，使$(1+a) N=(0)$。但$1+a \neq 0$（否则$1=-a \in I \Longrightarrow I=S$），$S$是整环，所以必有$N=(0)$。 ▎

当$\bigcap_{n=1}^{\infty} I^{n}=(0)$时，$S$不仅是Hausdorff空间，而且是一个度量空间。我们引入一个“距离”如下：令

$$v(x-y)=\sup \{n: x-y \in I^{n}\}.$$

应用$\bigcap I^{n}=(0)$，立得

$$v(x-y)=\infty \Longleftrightarrow x-y=0 \Longleftrightarrow x=y.$$

定义

$$d(x, y)=e^{-v(x-y)},$$

其中e为任意指定的大于1的实数。我们要验证$d(x, y)$适合下面的三个条件，因此是一个距离：

1）$d(x, y) \geqslant 0$，$d(x, y)=0 \Longleftrightarrow x=y$；

2）$d(x, y)=d(y, x)$；

3）(三角不等式） $d(x, z) \leqslant d(x, y)+d(y, z)$。

1)与2)两条是明显的。对于3)，我们要证明更强的3')：

3′)(**强三角不等式**)　$d(x,z)\leqslant \max(d(x,y),d(y,z))$。不难看出，3′)即是

$$v(x-z)\geqslant \min(v(x-y),v(y-z)).$$

事实上，设上式右端等于 l，则有

$$x-y,y-z\in I^{l}\Longrightarrow (x-y)+(y-z)\in I^{l}\Longrightarrow x-z\in I^{l}$$
$$\Longrightarrow v(x-y)\geqslant l.$$

在距离 $d(x,y)$ 作用下，S 是一个度量空间，而且由距离 $d(x,y)$ 引生的拓扑，即是原来的 I-adic 拓扑。

以上的讨论容易推广到 S 模 M 上去。

在任何度量空间 M 里，我们都可以取它的完备化集。其作法与第一章§6“p-adic 数与赋值”中的作法大同小异，我们略述如下。

M 的一个序列 $(m_1,m_2,\cdots,m_n,\cdots)$ 如适合下面的条件，则称为一个柯西序列：任给一个实数 $\varepsilon>0$，必存在一个正整数 $N(\varepsilon)$，使得

$$n,n'>N(\varepsilon)\Longrightarrow d(m_n,m_{n'})<\varepsilon.$$

两个柯西序列 $(m_1,m_2,\cdots,m_n,\cdots)$ 及 $(m_1',m_2',\cdots,m_n',\cdots)$ 称为等价的（记为 $(m_1,m_2,\cdots,m_n,\cdots)\sim(m_1',m_2',\cdots,m_n',\cdots)$），如果对于任一实数 $\varepsilon>0$，必存在一个正整数 $N(\varepsilon)$，使得

$$n>N(\varepsilon)\Longrightarrow d(m_n,m_n')<\varepsilon.$$

令 $C(M)$ 为 M 的所有柯西序列的集合。定义 $\hat{M}=C(M)/\sim$，则称 $\hat{M}$ 是 M 的完备化集。

设 S 为拓扑环，M 是拓扑模，S,M 都是度量空间。如上定义它们的完备化集 $\hat{S}$ 及 $\hat{M}$。我们可以看出 $\hat{S}$ 是环，S 是 $\hat{S}$ 的子环，S 到 $\hat{S}$ 的认同映射 σ 是如下定义的：

$$\sigma:\ s\to(s,s,\cdots,s,\cdots)\to\hat{S}.$$

并且 $\hat{M}$ 是 $\hat{S}$ 模。与第一章§6完全一样，我们可以证明 $\hat{S},\hat{M}$ 都是完备的，即

$$\hat{\hat{S}} = \hat{S}, \qquad \hat{\hat{M}} = \hat{M}.$$

定理6.36 设 S 是诺德环，M 是有限生成的 S 模，则

$$\hat{M} = \hat{S} \cdot M.$$

证明 设 $M = \sum_{i=1}^{r} Sm_i$. 任取 $\hat{m} \in \hat{M}$. 令

$$\hat{m} = [(m'_1, m'_2, \cdots, m'_n, \cdots)].$$

（即 $(m'_1, m'_2, \cdots, m'_m, \cdots)$ 在柯西序列集合 $C(M)$ 中所决定的等价类）．我们有

$$m'_{n+1} - m'_n \in I^{s_n} M,$$

其中 s_n 为正整数，且 $n \to \infty$ 时 $s_n \to \infty$. 不难看出

$$I^{s_n} M = \sum_{i=1}^{r} I^{s_n} m_i,$$

故

$$m'_{n+1} - m'_n = \sum_{i=1}^{r} a_{ni} m_i, \quad a_{ni} \in I^{s_n}.$$

令

$$m'_1 = \sum_{i=1}^{r} b_{1i} m_i, \qquad b_{1i} \in S,$$

立得

$$m'_n = m'_1 + (m'_2 - m'_1) + \cdots + (m'_n - m'_{n-1}) = \sum_{i=1}^{r} b_{ni} m_i,$$

其中

$$b_{ni} = b_{1i} + a_{1i} + \cdots + a_{n-1,i}.$$

不难看出 $(b_{1i}, b_{2i}, \cdots, b_{ni}, \cdots)$ 是 S 的一个柯西序列，故

$$\hat{m} = \sum_{i=1}^{r} [(b_{1i}, b_{2i}, \cdots, b_{ni}, \cdots)] m_i \in \sum_{i=1}^{r} \hat{S} m_i \subset \hat{S} m.$$

反之，显然有 $\hat{M} \supset \hat{S} M$. ▍

例21 考虑

$$\boldsymbol{Z}_{\mathfrak{p}}=\left\{\frac{m}{n}: n \bar{\in} \mathfrak{p}\right\},$$

此处 $\mathfrak{p}$ 是 $\boldsymbol{Z}$ 的一个素理想，$\mathfrak{p}=(p)$。又令 $\hat{\boldsymbol{Z}}_{\mathfrak{p}}$ 为 $\boldsymbol{Z}_{\mathfrak{p}}$ 对理想 $\mathfrak{p}$ 的完备化环，则 $\hat{\boldsymbol{Z}}_{\mathfrak{p}}$ 是 p-adic 整数环(参考第一章 § 6)。 ▎

考虑 $S=K[x_1,\cdots,x_n]$，$I=(x_1,\cdots,x_n)$。则 S 对 I 的完备化环为

$$\begin{aligned}\hat{S}&=K[[x_1,\cdots,x_n]]\\&=\{\sum a_{i_1 i_2\cdots i_n}x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}: a_{i_1 i_2\cdots i_n}\in K,\ i_j\geqslant 0\},\end{aligned}$$

即 K 上的 n 元**形式幂级数环**。

例如，取 $K=\boldsymbol{R}$ 或 $\boldsymbol{C}$，则下列都是形式幂级数

$$\sum_{n=0}^{\infty}x^n,\qquad \sum_{n=1}^{\infty}n^n x^n,\qquad \sum_{n=1}^{\infty}n^{-n}x^n,$$

它们分别是函数论中的收敛幂级数，发散幂级数及整函数。可是在我们的考虑之下，它们都叫形式幂级数。在函数论中被驱逐出境的发散幂级数，经过代数学又回到数学的领域了。 ▎

一个环 K 上的形式幂级数

$$f=\sum a_{i_1\cdots i_n}x_1^{i_1}\cdots x_n^{i_n},\qquad a_{i_1\cdots i_n}\in K$$

可能有无限多项，因此无最高次项，也没有次数。自然，它有首项，也有最低次数，称为**阶数**，记为 $v(f)$。它也就是我们在引入距离 $d(x,y)$ 时所用的

$$v(f)=\sup\{m: f\in(x_1,\cdots,x_n)^m\}.$$

一般地，我们有

1) $v(f)\geqslant 0$，$v(f)=\infty \Longleftrightarrow f=0$；

2) $v(f\cdot g)\geqslant v(f)+v(g)$；

3) $v(f+g)\geqslant \min(v(f),v(g))$。

当 $S=K[[x_1,\cdots,x_n]]$ 的常数环 K 是整环时，不难看出，2)被

下面的2′)所取代：

2′) $v(f\cdot g)=v(f)+v(g)$。

由1)及2′)，我们立刻导出：如果K是整环，则$K[[x_1,\cdots,x_n]]$也是整环。

如果K是诺德环，那么我们可以证明$K[[x_1,\cdots,x_n]]$也是诺德环。证法有二：一是仿照定理3.26(希尔伯特基定理)，只是我们要略加修改：令

$$I_n=\{a_n:\ a_nx^n+a_{n+1}x^{n+1}+\cdots\in I\}。$$

读者试自行完成这个证明；二是下面的定理6.39的系。

一般言之，如果S是整环，那么$\hat{S}$不一定是整环。我们以下面的例子来说明这个现象。

例22 设$S=\boldsymbol{R}[x,y]$，x,y适合下式：

$$xy-x^3-y^3=0。$$

读者试自证明，对变数X,Y而言，$f(X,Y)=XY-X^3-Y^3$是不可分解的。因此

$$S=\boldsymbol{R}(x,y)\approx\boldsymbol{R}[X,Y]/(f(X,Y))$$

是一个整环。令$I=(x,y)$，$\hat{S}$为S对I的完备化环。则

$$\hat{S}=\boldsymbol{R}[[x,y]],$$

而且x,y仍适合原来的等式：

$$xy-x^3-y^3=0。$$

故

$$\hat{S}=\boldsymbol{R}[[X,Y]]/(f(X,Y))。$$

可是，在$\boldsymbol{R}[[X,Y]]$中$f(X,Y)$是可以分解的，即

$$f(X,Y)=(X-Y^2+\cdots)(Y-X^2+\cdots),$$

所以，我们有

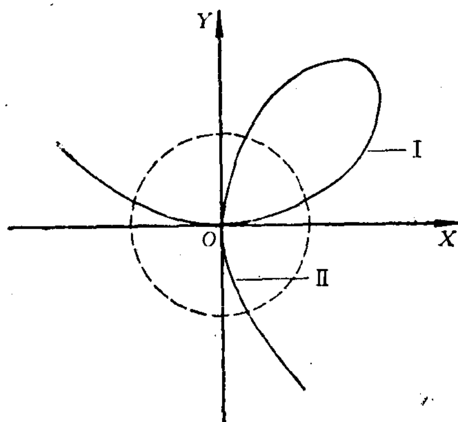
$$x-y^2+\cdots\neq 0,\qquad y-x^2+\cdots\neq 0,$$

但

$$(x-y^2+\cdots)(y-x^2+\cdots)=0,$$

因而$\boldsymbol{R}[[x,y]]$不是整环。

用几何图形来说明(见图6.2)，多项式$f(X,Y)=0$的解是一条代数曲线，而形式幂级数$f(X,Y)=0$的解是两条解析曲线。



Ⅰ：多项式$f(X,Y)=0$的解
Ⅱ：虚线内，相当于幂级数$f(X,Y)=0$的解

图 6.2

以下我们逐步证明，如果S是诺德环，那么$\hat{S}$也是诺德环。我们先证明：

定理6.37 设S是诺德环，I是理想，$\bigcap_{n=1}^{\infty} I^n=(0)$，$\hat{S}$是$S$对$I$-adic拓扑的完备化环，$\hat{I}=I\hat{S}$（见上定理），$G_I(S)$是$S$的与理想$I$相伴的分次环，$G_{\hat{I}}(\hat{S})$是$\hat{S}$的与理想$\hat{I}$相伴的分次环。那么，我们恒有

$$G_I(S)\approx G_{\hat{I}}(\hat{S}).$$

证明 因为$\hat{I}^i=(I\hat{S})^i=I^i\hat{S}$ $(i=0,1,2,\cdots)$，所以

$$I^i\cap \hat{I}^{i+1}=I^{i+1}.$$

考虑映射

$$I^i \xrightarrow{\tau} \hat{I}^i \xrightarrow{\sigma} \hat{I}^i/\hat{I}^{i+1},$$

其中τ为认同映射，σ为典型映射。显然，上面的映射引生出的

$$\sigma: I^i/I^{i+1}(=I^i/I^i\cap\hat{I}^{i+1})\longrightarrow\hat{I}^i/\hat{I}^{i+1}$$

是单射。任取 $\hat{b}=[(b_1,\cdots,b_n,\cdots)]\in\hat{I}^i$，则存在 $b\in S$，使

$$[(b_1,\cdots,b_n,\cdots)-(b,\cdots,b,\cdots)]\in\hat{I}^{i+1}.$$

于是 $b=[(b,\cdots,b,\cdots)]\in\hat{I}^i\cap S=I^i$，且

$$\sigma(b)=\sigma(b_1,\cdots,b_n\cdots).$$

所以 σ 是满射，也即 $I^i/I^{i+1}\approx\hat{I}^i/\hat{I}^{i+1}$。自然

$$G_I(S)=\oplus I^i/I^{i+1}\approx\oplus\hat{I}^i/\hat{I}^{i+1}=G_{\hat{I}}(\hat{S}).\ \blacksquare$$

我们以前已证明，如果 S/I 是诺德环，I 是有限生成的理想，那么 $G_I(S)$ 也是诺德环。现在我们要推出部分逆定理。

定理6.38 条件如上定理。设 M 是 $\hat{S}$ 模。如果 $G_{\hat{I}}(M)$ 是有限生成的 $G_{\hat{I}}(\hat{S})$ 模，则 M 是有限生成的 $\hat{S}$ 模。

证明 令 $(\bar{m}_1,\cdots,\bar{m}_n)$ 是 $G_{\hat{I}}(M)$ 的一个齐次生成元集，$\bar{m}_i\in\hat{I}^{e_i}M/\hat{I}^{e_i+1}M$。设 $m_i\in\hat{I}^{e_i}M$，使得 $m_i+\hat{I}^{e_i+1}=\bar{m}_i$。我们要证明 $\{m_1,\cdots,m_n\}$ 是 M 的一生成元集。任取 $m\in M$，设 $m\in\hat{I}^{n_1}M$，则 $\bar{m}\in\hat{I}^{n_1}M/\hat{I}^{n_1+1}M$ 可以写成

$$\bar{m}=\sum_{i=1}^{n}a_{n_1i}\bar{m}_i,\quad a_{n_1i}\in\hat{I}^{n_1-e_i}.$$

于是

$$m^{(1)}=m-\sum_{i=1}^{n}a_{n_1i}m_i\in\hat{I}^{n_2}M\subset\hat{I}^{n_1+1}M.$$

再令

$$\bar{m}^{(1)}=\sum_{i=1}^{n}a_{n_2i}\bar{m}_i,\quad a_{n_2i}\in\hat{I}^{n_2-e_i}.$$

依此类推。因为 $\hat{S}$ 是完备的，所以

$$a_i=\sum_{j=1}^{\infty}a_{n_ji}\in\hat{S}.$$

我们考虑

$$m-\sum_{i=1}^{n}a_i m_i\in \hat{I}^{n_j}M,\qquad n_j\to\infty,$$

立得

$$m-\sum_{i=1}^{n}a_i m_i\in \bigcap_{j=1}^{\infty}\hat{I}^{n_j}=\{0\}. \quad \blacksquare$$

定理6.39 条件如定理6.37. 我们恒有 $\hat{S}$ 是诺德环.

证明 S 是诺德环$\Longrightarrow G_I(S)$是诺德环 $\Longrightarrow G_{\hat{I}}(\hat{S})$是诺德环（在上定理中取 M 为 $\hat{S}$ 的任一理想）$\Longrightarrow \hat{S}$ 是诺德环. $\blacksquare$

系 设 K 是诺德环, 则 $K[[x_1,\cdots,x_n]]$是诺德环, 此处 $x_1,\cdots,x_n$ 是变数.

证明 令 $S=K[x_1,\cdots,x_n]$, $I=(x_1,\cdots,x_n)$. 那么, S 对 I 的完备化环 $\hat{S}=\mathrm{K}[[x_1,\cdots,x_n]]$. $\blacksquare$

我们现在回到形式幂级数环 $K[[x_1,\cdots,x_n]]$的讨论. 在§3中, 我们建立了多项式环 $K[x_1,\cdots,x_n]$与仿射空间 K^n 的联系, 此处 K 是一个代数封闭域. 我们能用同样的方法, 用 $K[[x_1,\cdots,x_n]]$建立几何学吗? 问题是对任意的 $f\in K[[x_1\cdots,x_n]]$, $f=0$可能无解(f 是可逆的) 或 $f=0$仅有原点$(0,\cdots,0)$为唯一解(f 是发散的). 例如

$$f(x_1,x_2)==\sum(i_1+i_2)^{i_1+i_2}x_1^{i_1}x_2^{i_2}.$$

如果我们用§4的谱集, 则可避免这些困难. 另外一个方法, 设 $K=\boldsymbol{R}$ 或 $\boldsymbol{C}$(或下一章所谈到的“赋值域”), 那么我们可以考虑介于 $K[x_1,\cdots,x_n]$与 $K[[x_1,\cdots,x_n]]$之间的**收敛幂级数环** $K\{\{x_1,\cdots,x_n\}\}$, 其定义如下:

$$K\{\{x_1,\cdots,x_n\}\}=\{\sum a_{i_1\cdots i_n}x_1^{i_1}\cdots x_n^{i_n}: \text{存在 } A,B\in\boldsymbol{R}, \text{ 使得 } |a_{i_1\cdots i_n}|\leqslant AB^{i_1+\cdots+i_n}\}.$$

此时,我们可以用 $K\{\{x_1,\cdots,x_n\}\}$建立解析几何. 请注意,$K\{\{x_1,$

$\cdots,x_n\}\}$对理想$(x_1,\cdots,x_n)$的完备化集，也是$K[[x_1,\cdots,x_n]]$。

应用下面的恒等式：

$$\frac{1}{1-x}=1+x+x^2+\cdots+x^n+\cdots,$$

我们立刻可以知道$K[[x_1,\cdots,x_n]]$中的可逆元。事实上，$f(x_1,\cdots,x_n)$是可逆元$\Longleftrightarrow f(0,\cdots,0)$是$K$的可逆元(在$K$是域的情形下，这就是说$f(0,\cdots,0)\neq 0$)。证明如下：

$\Longrightarrow$。设$f(x_1,\cdots,x_n)$可逆，则有$g(x_1,\cdots,x_n)$，使

$$f(x_1\cdots,x_n)\cdot g(x_1,\cdots,x_n)=1,$$

即有$f(0,\cdots,0)g(0,\cdots,0)=1$。

$\Longleftarrow$。令

$$f(x_1,\cdots,x_n)=a+g(x_1,\cdots,x_n),\quad g(0,\cdots,0)=0.$$

则

$$f(x_1,\cdots,x_n)=a(1-h(x_1,\cdots,x_n)),\quad h(0,\cdots,0)=0.$$

于是
$$f^{-1}=a^{-1}\left(1+\sum_{i=1}^{\infty}(h(x_1,\cdots,x_n))^i\right).$$

其中
$$v(h^i)\geqslant iv(h)\to\infty,\quad 当\ i\to\infty.$$

所以$f^{-1}\in K[[x_1,\cdots,x_n]]$。

我们有下面的重要定理。

定理6.40 (Weierstrass**预备定理**) 设K是域，$f(x_1,\cdots,x_n)\in K[[x_1,\cdots,x_n]]$，$f(0,\cdots,0,x_n)\neq 0$。换句话说，$f(x_1,\cdots,x_n)$中有一项$ax_n^h$，$a\in K$，$a\neq 0$。那么

1) 任给$g(x_1,\cdots,x_n)\in K[[x_1,\cdots,x_n]]$，必存在唯一的$d\in K[[x_1,\cdots,x_n]]$及$r\in K[[x_1,\cdots,x_{n-1}]][x_n]$，使

$$g=df+r,\quad v(f(0,\cdots,0,x_n))>\deg_{x_n}r.$$

2) 存在唯一的可逆元$\delta\in K[[x_1,\cdots,x_n]]$及对$x_n$为首一多项式的$f^*\in K[[x_1,\cdots,x_{n-1}]][x_n]$，使

$$f=\delta f^*,\quad v(f(0,\cdots,0,x_n))=\deg_{x_n}f^*.$$

证明 1) **唯一性。** 设有 $g=df+r=d'f+r'$。则

$$(d-d')f=r'-r.$$

假若 $r'-r\neq 0$，则有

$$\begin{aligned}
&v((d(0,\cdots,0,x_n)-d'(0,\cdots,0,x_n))\cdot f(0,\cdots,0,x_n))\\
&\quad =v(d(0,\cdots,0,x_n)-d'(0,\cdots,0,x_n))+v(f(0,\cdots,0,x_n))\\
&\quad >\deg_{x_n}(r'-r)\geqslant v(r'(0,\cdots,0,x_n)-r((0,\cdots,0,x_n)),
\end{aligned}$$

这与$(d-d')f=r'-r$ 矛盾。故必有 $r=r'$，也即有 $d=d'$。

存在性。 令 $R=K[[x_1,\cdots,x_{n-1}]]$，$\mathfrak{m}=(x_1,\cdots,x_{n-1})R$。设

$$f=\sum_{i\geq 0}f_ix_n^i,\quad f_i\in R;$$

$$l=v(f(0,\cdots,0,x_n));$$

$$f'=\sum_{0\leq i<l}f_ix_n^i,\qquad f^*=\left(\sum_{i\geq l}f_ix_n^i\right)\Big/x_n^l=\sum_{i\geq l}f_ix_n^{i-l}.$$

则 $f'\in\mathfrak{m}[x_n]$，f^* 是 $R[[x_n]]=K[[x_1,\cdots,x_n]]$的可逆元。又令

$$\bar{f}=-f'/f^*,$$

则 $\bar{f}\in\mathfrak{m}[[x_n]]$，且有

$$f=f'+x_n^lf^*=(x_n^l-\bar{f})f^*.$$

为证明存在性，我们只须找到一个 $d\in K[[x_1,\cdots,x_n]]$，使

$$g-df\in R[x_n],$$

且

$$\deg_{x_n}(g-df)<l.$$

也即只须找到一个 $\bar{d}(=f^*d)$，使得

$$\deg_{x_n}(\bar{g}-(x_n^l-\bar{f})\bar{d})<l,$$

这里 $\bar{g}=g$，即任意给定的幂级数。我们由 $\bar{g}$ 及 $\bar{f}$ 去逐步求解 $\bar{d}$ 如下：设

$$(1)\qquad \bar{g}=\sum_i g_ix_n^i\quad(g_i\in R),\qquad \bar{f}=\sum\bar{f}_ix_n^i\quad(\bar{f}_i\in\mathfrak{m}).$$

令 $u=0,1,2,\cdots$。我们归纳地定义

$$(2)\qquad d_{0e}=g_{l+e},\qquad \forall e\geqslant 0,$$

$$(3)\qquad d_{u+1,e}=\sum_{j=0}^{l+e}\bar{f}_j d_{u,l+e-j},\qquad \forall u\geqslant 0,\ e\geqslant 0$$

$$(4)\qquad d_u=\sum_{e\geqslant 0}d_{ue}x_n^e,\qquad \forall u\geqslant 0.$$

那么，易于看出

$$(5)\qquad \deg_{x_n}(\bar{g}-d_0x_n^l)<l,$$

$$(6)\qquad \deg_{x_n}(-d_{u+1}x^l+d_u\bar{f})<l,\qquad \forall u\geqslant 0.$$

由于 $\bar{f}_j\in\mathfrak{m}$，不难逐步得出

$$d_{ue}\in\mathfrak{m}^u,\qquad \forall u\geqslant 0,\ e\geqslant 0.$$

令

$$\bar{d}=\sum_{u\geqslant 0}d_u=\sum_{u\geqslant 0}\sum_{e\geqslant 0}d_{ue}x_n^e$$

$$=\sum_{e\geqslant 0}\left(\sum_{u\geqslant 0}d_{ue}\right)x_n^e=\sum_{e\geqslant 0}d_e^*x_n^e,$$

此处 $d_e^*=\sum_{u\geqslant 0}d_{ue}\in R$。显然，利用(5)与(6)二式及下式

$$\bar{g}-d_0x_n^l+\sum_{u=0}^{\infty}(-d_{u+1}x_n^l+d_u\bar{f})=\bar{g}-(x_n^l-\bar{f})\bar{d},$$

即知 $\bar{d}$ 符合我们的要求。本定理的前半部得证。

2）同 1)一样的，令 $l=v(f(0,\cdots,0,x_n))$。应用 1)，令 $g=x_n^l$，于是有

$$x_n^l=df+r,\qquad r\in R[x_n],\ \deg_{x_n}r<l.$$

即

$$x_n^l-r=df.$$

在上式中，令 $x_1=x_2=\cdots=x_{n-1}=0$，比较两侧 x_n 的阶 v，立得

$$l\geqslant v(x_n^l-r(0,\cdots,0,x_n))=v(df)$$

$$=v(d(0,\cdots,0,x_n))+l.$$

于是必有

$$v(d(0,\cdots,0,x_n))=0.$$

故有

$$d(0,\cdots,0,x_n)=a+\sum_{i=1}^{\infty}a_i x_n^i,\quad a,a_i\in K,\ a\neq 0.$$

所以

$$d(0,\cdots,0,0)=a\neq 0,$$

也即 $d(x_1,\cdots,x_n)$是可逆元。我们令

$$d^{-1}=\delta,\ x_n^l-r=f^*,$$

即得本定理的 2)。 ▎

讨论 1) 上面这个定理，把形式幂级数环 $K[[x_1,\cdots,x_n]]$ 代数化了。仿此可以证明收敛幂级数环 $K\{\{x_1,\cdots,x_n\}\}$的Weierstrass 预备定理。许多解析几何的定理都可以从这里导出。例如，设 $K=\boldsymbol{C}$，任取 $f\in \boldsymbol{C}\{\{x_1,\cdots,x_n\}\}$，令

$$f=f_l(x_1,\cdots,x_n)+f_{l+1}(x_1,\cdots,x_n)+\cdots,$$

此处 f_i 是 i 次齐次式。如果适当地选取坐标

$$y_j=\sum_{i=1}^{n}a_{ji}x^i,$$

不难看出，我们可以假设

$$f_l(0,\cdots,0,x_n)=ax_n^l\quad(a\neq 0).$$

于是，根据 Weierstrass 预备定理，可得

$$f=\delta f^*,$$

其中 δ 可逆，

$$f^*=x_n^l+\sum_{i=1}^{l}f_i^*(x_1,\cdots,x_{n-1})x_n^{l-i}.$$

在原点附近，$\delta\neq 0$，所以

$$f=0\Longrightarrow f^*=0.$$

易于看出，任取 $x_1,\cdots,x_{n-1}$ 充分接近0，则由$f^*=0$可以解出 l 个

x_n的值。这就是说，在原点附近，$f^*=0$的解形成一个解析多样体，而它是C^{n-1}的原点的一个邻域的l次覆盖(可能有分支点)。

2) 从代数的观点来看，立得

$$K[[x_1,\cdots,x_n]]/(f)=K[[x_1,\cdots,x_n]]/(f^*),$$

所以它是$K[[x_1,\cdots,x_{n-1}]]$的一个整数扩充。请与诺德正规化定理相比较。

习　题

1. 令$S=R[x_1,x_2,\cdots,x_n]$，其中R为环，$I=(x_1,x_2,\cdots,x_n)$。证明S的I-adic完备化环为

$$\hat{S}=R[[x_1,x_2,\cdots,x_n]].$$

2. 令$S=K[x_1,x_2,\cdots,x_n]_{(x_1,x_2,\cdots,x_n)}$，其中$K$为域，$I=(x_1,x_2,\cdots,x_n)$。证明$S$的$I$-adic完备化环为

$$\hat{S}=K[[x_1,x_2,\cdots,x_n]].$$

3. 令$S=\mathbf{Z}_{(p)}$，其中p为素数。令$\hat{\mathbf{Z}}_{(p)}$为S的p-adic完备化环。证明$\hat{\mathbf{Z}}_{(p)}$的比域为$\mathbf{Q}_p$(参见第一章§6)。

4. 设R是诺德环，I是R的理想，R的I-adic完备化环记为$\hat{R}$。对$x\in R$，以$\hat{x}$表示x在认同映射$R\to\hat{R}$下的象。证明x不是R的零因子$\Longrightarrow\hat{x}$不是$\hat{R}$的零因子。

5. 令$R=\mathbf{C}[x,y]/(x^2-y^2-y^3)$，$I=(\bar{x},\bar{y})$。证明$R$是整环，但它的$I$-adic完备化环$\hat{R}$不是整环。

6. 设R是诺德局部环，$\mathfrak{m}$是R的极大理想。证明$\hat{\mathfrak{m}}$是$\hat{R}$的极大理想。

7. 设R是环，I是R的理想，$S=1+I$，则S是R的乘法封闭子集。证明环映射

$$f: S^{-1}R\to\hat{R},$$

$$\frac{r}{1+a}\mapsto r(1-a+a^2-\cdots)$$

(其中$a\in I$)是嵌入。

8. 设R是诺德环，I是R的理想，M是有限R模。证明

$$\bigcap_{n=1}^{\infty} I^n M = \bigcap_{\mathfrak{m}} \ker(f_{\mathfrak{m}}),$$

其中$f_{\mathfrak{m}}$表示M到$M_{\mathfrak{m}}$的认同映射，上式右端的交是对所有包括I的极大理想$\mathfrak{m}$取的。

9. 设R是环，I是R的理想，M,N,S都是R模，且

$$0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} S \longrightarrow 0$$

正合。证明在I-adic拓扑下，f,g诱导出$\hat{R}$模映射$\hat{f},\hat{g}$，使得

$$0 \longrightarrow \hat{M} \xrightarrow{\hat{f}} \hat{N} \xrightarrow{\hat{g}} \hat{S} \longrightarrow 0$$

正合。

10. 举例说明诺德环R上的非有限生成模M在I-adic拓扑下的完备化不一定等于$\hat{R}M$(这里I是R的一个理想)。

11. 令$f(x,y)=y^2+y^3+xy+x^4$。参考Weierstrass预备定理，求$\delta(x,y),a_1(x),a_2(x)$的次数小于3的项，适合

$$f(x,y)=\delta(x,y)(y^2+a_1(x)y+a_2(x)).$$

§9 维数论(2)

在§6中，我们讨论了维数，并证明了定理6.26：

$$\dim S=\sup\{\dim S_{\mathfrak{m}}: \mathfrak{m}\text{ 是极大理想}\}.$$

因此，维数被局部化了，了解一个局部环的维数是很重要的。

在§7中，对于一个局部环S，我们讨论了分次环$G_{\mathfrak{m}}(S)$，此处$\mathfrak{m}$是S的极大理想。当我们把$G_{\mathfrak{m}}(S)$当作$G_{\mathfrak{m}}(S)$模时，又得出了它的Hilbert特征多项式$\chi_{\mathfrak{m}}^S(x)$。我们曾用例子指明$d=\deg \chi_{\mathfrak{m}}^S(x)$即是维数。在本节中，我们将对局部环$S$，给出证明。先引入下面的定义。

定义6.19 设S是一个诺德局部环，$\mathfrak{m}$是它的极大理想。又设I是一个准素理想，$\sqrt{I}=\mathfrak{m}$，则称I是S的一个**定义理想**。

讨论 1）根据希尔伯特零点定理，

$$\mathscr{V}(I)=\mathscr{V}(\sqrt{I})=\mathscr{V}(\mathfrak{m})=\{\mathfrak{m}\}.$$

2）令 $\mathfrak{m}=(m_1,\cdots,m_n)$，$m_i^{s_i}\in I$。那么，当 s 足够大时，显然有 $\mathfrak{m}^s\subset I\subset\mathfrak{m}$。反之，如果存在 s，使 $\mathfrak{m}^s\subset I\subset\mathfrak{m}$，则 I 是准素理想，$\sqrt{I}=\mathfrak{m}$。即：

$$I\text{ 是定义理想}\Longleftrightarrow\text{对某个 }s,\ \mathfrak{m}^s\subset I\subset\mathfrak{m}.$$

3）I 是定义理想 $\Longleftrightarrow I\subset\mathfrak{m}$，且 S/I 是 Artin 环。说明：$\Longrightarrow$。令 $\bar{\mathfrak{p}}$ 是 S/I 的素理想，则 $\mathfrak{p}\supset I\supset\mathfrak{m}^s$，故

$$\mathfrak{p}=\sqrt{\mathfrak{p}}\supset\sqrt{\mathfrak{m}^s}=\mathfrak{m},$$

即有 $\dim(S/I)=0$，所以 S/I 是 Artin 环。$\Longleftarrow$。取 I 的简略准素分解 $I=\bigcap I_i$。如果有 $\mathfrak{p}_i=\sqrt{I_i}\neq\mathfrak{m}$，则 $\bar{\mathfrak{p}}_i\subsetneqq\bar{\mathfrak{m}}$，因此 $\dim(S/I)\geqslant 1$。这是不可能的。所以 I 的简略准素分解必然是 $I=I$，$\sqrt{I}=\mathfrak{m}$，I 是准素理想。

引理 设 $J,I_1,\cdots,I_n$ 是环 S 的理想，而且最多只有两个 I_i 不是素理想。那么，$J\subset\bigcup I_i\Longrightarrow$存在一个 i，使 $J\subset I_i$。

证明 我们对 n 取归纳法。$n=1$ 时，本引理显然是正确的。我们现在考虑 $n>1$ 的情形。如果存在某个 j，使得

$$J\subset\bigcup_{i\neq j}I_i,$$

那么用归纳法，立得本引理。因此，只须考虑下面的情形：

$$J\not\subset\bigcup_{i\neq j}I_i,\qquad j=1,2,\cdots,n.$$

现在证明这是不可能的。

若发生上述情形，则存在

$$a_j\in J\setminus\bigcup_{i\neq j}I_i\quad(j=1,2,\cdots,n).$$

已知 $J\subset\bigcup I_i$，立得 $a_j\in I_j$。如果 $n=2$，我们得到

$$a_1+a_2\in J\subset I_1\cup I_2.$$

于是 $a_1+a_2\in I_1\Longrightarrow a_2\in I_1$. $a_1+a_2\in I_2\Longrightarrow a_1\in I_2$。两者都与

a_1,a_2的选法相违，因此是不可能的。设$n>2$，那么至少有一个I_i是素理想，不妨设I_1是素理想。考虑下面的元素

$$b=a_1+a_2a_3\cdots a_n\in J,$$

于是，$a_1\in I_1$，$a_2,\cdots,a_n\notin I_1\Longrightarrow b\notin I_1$。任取$j>1$，则

$$a_1\notin I_j,\ a_2\cdots a_n\in I_j\Longrightarrow b\notin I_j,$$

所以$J\ni b\notin\bigcup I_j$。这是一个矛盾。▌

讨论 如果环$S\supset K$，K是无限域，那么在上面的引理中，不需要假定任何I_i是素理想。此时，S,J,I都是K向量空间。$J=J\cap(\bigcup I_i)=\bigcup(J\cap I_i)$。当$J\cap I_i\neq J$时，$J$不可能是子空间$J\cap I_i$ $(i=1,\cdots,n)$的并集。

定理6.41 设S是诺德局部环，m是它的极大理想。则下面三个数字是相同的：

1) $\dim S$;

2) 任取S的一个定义理想I，S对I的Hilbert特征多项式$\chi_I^S(x)$的次数$d(S)=d$;

3) $n=\inf\{h:(a_1,\cdots,a_h)$是$S$的一个定义理想$\}$。

证明 首先我们要说明，2)中的d与定义理想I的选取无关。这只须说明

$$\deg\chi_{\mathfrak{m}}^S(x)=\deg\chi_I^S(x)$$

就可以了。事实上，由于I是定义理想，所以有正整数s，使$\mathfrak{m}^s\subset I\subset\mathfrak{m}$。故对任意正整数$i$，有

$$l(S/\mathfrak{m}^{si})\geqslant l(S/I^i)\geqslant l(S/\mathfrak{m}^i).$$

而当i足够大以后，我们有$\chi_{\mathfrak{m}}^S(i)=l(S/\mathfrak{m}^i)$及$\chi_I^S(i)=l(S/I^i)$，所以

$$\chi_{\mathfrak{m}}^S(si)\geqslant\chi_I^S(i)\geqslant\chi_{\mathfrak{m}}^S(i).$$

令$i\to\infty$，即知$\deg\chi_{\mathfrak{m}}^S(x)=\deg\chi_I^S(x)$。

下面我们证明$d\geqslant\dim S\geqslant n\geqslant d$，以完成本定理的证明。

1) 证明$d\geqslant\dim S$。对d作归纳法。设$d=0$，则当i足够大时，

$$l(S/I^t)=\sum_{i=0}^{t-1} l(I^i/I^{i+1})$$

是常数。于是 $l(I^t/I^{t+1})=0$，即 $I^t=I^{t+1}$。应用 Nakayama 引理，立得 $I^t=(0)$。由于 I 是定义理想，故有正整 s，使 $\mathfrak{m}^s\subset I$，于是，$\mathfrak{m}^{st}\subset I^t=(0)$。根据定理6.29的系，$S$ 是 Artin 环，即得

$$\dim S = 0 \leqslant d.$$

现在讨论 $d>0$ 的情形。任取 S 的一个素理想链

$$\mathfrak{m}=\mathfrak{p}_0\supsetneqq\mathfrak{p}_1\supsetneqq\cdots\supsetneqq\mathfrak{p}_l,$$

我们只要证明 $l\leqslant d$ 就足够了。考虑 $S/\mathfrak{p}_l$，这是一个整环及局部环，它的极大理想是 $\mathfrak{m}/\mathfrak{p}_l$。同时我们有

$$(\mathfrak{m}/\mathfrak{p}_l)^r=(\mathfrak{m}^r+\mathfrak{p}_l)/\mathfrak{p}_l,$$

$$(S/\mathfrak{p}_l)/(\mathfrak{m}/\mathfrak{p}_l)^r=(S/\mathfrak{p}_l)/((\mathfrak{m}^r+\mathfrak{p}_l)/\mathfrak{p}_l)\approx S/(\mathfrak{m}^r+\mathfrak{p}_l).$$

于是

$$l((S/\mathfrak{p}_l)/(\mathfrak{m}/\mathfrak{p}_l)^r)=l(S/(\mathfrak{m}^r+\mathfrak{p}_l))\leqslant l(S/\mathfrak{m}^r).$$

也即 $d(S/\mathfrak{p}_l)\leqslant d(S)$。另一方面，

$$\mathfrak{m}/\mathfrak{p}_l=\mathfrak{p}_0/\mathfrak{p}_l\supsetneqq\mathfrak{p}_1/\mathfrak{p}_l\supsetneqq\cdots\supsetneqq\mathfrak{p}_l/\mathfrak{p}_l=(0)$$

是 $S/\mathfrak{p}_l$ 的一个素理想链。显然，

$$l\leqslant d(S/\mathfrak{p}_l)\Longrightarrow l\leqslant d(S)=d.$$

所以我们不妨假定 $\mathfrak{p}_l=(0)$，S 是一个整环。现在，利用这个假定，继续我们的证明。任取 $a\in\mathfrak{p}_{l-1}$，$a\neq 0$。考虑 $S/aS=R$。显然

$$\mathfrak{m}/aS\supsetneqq\mathfrak{p}_1/aS\supsetneqq\cdots\supsetneqq\mathfrak{p}_{l-1}/aS$$

是 R 的一个素理想链，它的长度是 $l-1$。如果我们能证明

$$d(R)\leqslant d(S)-1=d-1,$$

那么，应用归纳法假设，立得

$$l-1\leqslant d(R)\leqslant d-1,\quad l\leqslant d.$$

下面证明 $d(R)\leqslant d(S)-1$。我们有下面的算式：

$$\begin{aligned}l((S/aS)/(\mathfrak{m}/aS)^r)&=l(S/(\mathfrak{m}^r+aS))\\&=l(S/\mathfrak{m}^r)-l((\mathfrak{m}^r+aS)/\mathfrak{m}^r)\end{aligned}$$

$$=l(S/\mathfrak{m}^r)-l(aS/\mathfrak{m}^r\cap aS).$$

应用定理 6.34(Artin-Rees 引理)，存在一 k，使

$$\mathfrak{m}^r\cap aS=\mathfrak{m}^{r-k}(\mathfrak{m}^k\cap aS)\subset a\mathfrak{m}^{r-k}.$$

于是
$$l(aS/\mathfrak{m}^r\cap aS)\geqslant l(aS/a\mathfrak{m}^{r-k}).$$

另一方面，我们已设 S 是整环，$a\neq 0$，所以映射

$$a^*: S\to aS,$$
$$a^*(b)=ab$$

是一个模同构。因此 $aS/a\mathfrak{m}^{r-k}\approx S/\mathfrak{m}^{r-k}$。于是，得出

$$l((S/aS)/(\mathfrak{m}/aS)^r)\leqslant l(S/\mathfrak{m}^r)-l(aS/a\mathfrak{m}^{r-k})$$
$$=l(S/\mathfrak{m}^r)-l(S/\mathfrak{m}^{r-k})=\chi_{\mathfrak{m}}^S(r)-\chi_{\mathfrak{m}}^S(r-k).$$

已知 $\chi_{\mathfrak{m}}^S(x)$ 是 d 次多项式，显然上面的差最多是 r 的 $d-1$ 次多项式。因此我们得出

$$d(R)=d(S/aS)\leqslant d(S)-1.$$

2) 证明 $\dim S\geqslant n$。前面已证 $\dim S\leqslant d<\infty$。对 $\dim S$ 取归纳法。设 $\dim S=0$，那么 S 是 Artin 环。应用定义 6.19 的讨论 3)，(0)是 S 的定义理想。按照通常的约定，空集 $\varnothing$ 生成 (0)。因此 $n=0$，$\dim S\geqslant n$。

现在考虑 $\dim S>0$ 的情形。令 $\mathfrak{p}_1,\cdots,\mathfrak{p}_r$ 是 S 的所有的极小素理想(参看定理 6.22 的讨论 4))。应用上面的引理，$\mathfrak{m}\not\subset\bigcup_{i=1}^r\mathfrak{p}_i$。令

$$a\in\mathfrak{m},\quad a\notin\bigcup_{i=1}^r\mathfrak{p}_i,\quad R=S/aS.$$

我们先证明 $\dim R\leqslant\dim S-1$。任取 R 的一个素理想链

$$\mathfrak{p}_0'/aS\supsetneqq\mathfrak{p}_1'/aS\supsetneqq\cdots\supsetneqq\mathfrak{p}_l'/aS,$$

此处 $\mathfrak{p}_i'$ 是 S 的包含 aS 的素理想。那么 $\mathfrak{p}_l'$ 必然包含一个极小素理想 $\mathfrak{p}_i$。又因为 $a\in\mathfrak{p}_l'$，$a\notin\mathfrak{p}_i$，所以 $\mathfrak{p}_l'\supsetneqq\mathfrak{p}_i$。于是

$$\mathfrak{p}_0'\supsetneqq\mathfrak{p}_1'\supsetneqq\cdots\supsetneqq\mathfrak{p}_l'\supsetneqq\mathfrak{p}_i$$

是 S 的一个素理想链。我们得出 $\dim R\leqslant\dim S-1$。

应用归纳法假设于 R，立得 R 有一定义理想 I/aS，其生成

元个数不超过 $\dim R=k$。设此生成元集为 $\{\bar{a}_1,\cdots,\bar{a}_k\}$，其中 $a_i\in S(i=1,\cdots,k)$。不难看出 I 是 S 的定义理想，$I=(a,a_1,\cdots,a_k)$，其生成元集的基数 $\leqslant \dim R+1\leqslant \dim S$。

3）证明 $n\geqslant d$。定理 6.33 已证过。▌

系1 任何诺德局部环 S 的维数 $\dim S$ 都是有限的。

系2 诺德环 S 的素理想的下降的链必然终止。

证明 任取一个素理想的下降的链

$$\mathfrak{p}_0\supsetneqq\mathfrak{p}_1\supsetneqq\cdots\supsetneqq\mathfrak{p}_n\supsetneqq\cdots.$$

对 $\mathfrak{p}_0$ 局部化。在诺德局部环 $S_{\mathfrak{p}_0}$ 里，我们有素理想链

$$\mathfrak{p}_0S_{\mathfrak{p}_0}\supsetneqq\mathfrak{p}_1S_{\mathfrak{p}_0}\supsetneqq\cdots\supsetneqq\mathfrak{p}_nS_{\mathfrak{p}_0}\supsetneqq\cdots.$$

所以它的长度 $\leqslant\dim S_{\mathfrak{p}_0}<\infty$。▌

从上面的定理，我们得出下面的富有几何意味的定理。

定理6.42(Krull 主理想定理) 1）设 I 是诺德环 S 的理想，$I\neq S$，I 由 n 个元素所生成。那么，令 $\mathfrak{p}$ 是一个包含 I 的素理想中的极小者，则有 $\mathrm{ht}(\mathfrak{p})\leqslant n$。

2）设 a 是诺德环 S 的不可逆元。那么，令 $\mathfrak{p}$ 是包含 (a) 的素理想中的极小者，则有 $\mathrm{ht}(\mathfrak{p})\leqslant 1$。

证明 显然，2)是 1)的特例。我们仅须证明 1)。考虑局部环 $S_{\mathfrak{p}}$。不难看出，$\mathfrak{p}S_{\mathfrak{p}}$ 既是包含 $IS_{\mathfrak{p}}$ 的素理想中的极小者，又是 $S_{\mathfrak{p}}$ 的极大理想，因此是唯一包含 $IS_{\mathfrak{p}}$ 的素理想。用 $IS_{\mathfrak{p}}$ 的简略准素分解，立即导出 $IS_{\mathfrak{p}}$ 是准素理想，以及

$$\sqrt{IS_{\mathfrak{p}}}=\mathfrak{p}S_{\mathfrak{p}},$$

故 $IS_{\mathfrak{p}}$ 是 $S_{\mathfrak{p}}$ 的定义理想。而 $IS_{\mathfrak{p}}$ 是由 n 个元素生成的，应用定理6.40，立得

$$\mathrm{ht}(\mathfrak{p})=\dim S_{\mathfrak{p}}\leqslant n.\ ▌$$

讨论 在 $\mathbf{C}[x_1,\cdots,x_n]=S$ 中，任取 $f\notin\mathbf{C}$，应用上面的定理，立得 $\mathrm{ht}((f))\leqslant 1$。但是在 S 中只有(0)的高度是 0，所以

$$\mathrm{ht}((f))=1.$$

令 $\mathfrak{p}_1,\cdots,\mathfrak{p}_l$ 是 (f) 的孤立素理想，则

$$\mathrm{ht}(\mathfrak{p}_i)=1, \quad \mathscr{V}((f))=\bigcup\mathscr{V}(\mathfrak{p}_i).$$

以 codim 表示余维数(参见定义6.13的讨论)，则

$$\operatorname{codim}\mathscr{V}(\mathfrak{p}_i)=ht(\mathfrak{p}_i)=1,$$

故
$$\dim\mathscr{V}(\mathfrak{p}_i)=n-\operatorname{codim}\mathscr{V}(\mathfrak{p}_i)=n-1.$$

这就是说，$f=0$ 的解集是一些**超曲面**的并集。这即证明了我们的一个几何直观。▌

设 S 是诺德局部环，$\mathfrak{m}$是它的极大理想，$d=\dim S$。那么存在一个定义理想 $I=(x_1,\cdots,x_d)$。任何一组如此的$\{x_1,\cdots,x_d\}$称为S的一个**参数系**。

令

$$K=S/\mathfrak{m},$$

则K是域。于是$\mathfrak{m}/\mathfrak{m}^2$是一个$K$向量空间。令$\{\bar{a}_1,\cdots,\bar{a}_n\}$是向量空间$\mathfrak{m}/\mathfrak{m}^2$的一组基(其中 $a_i\in\mathfrak{m}$，$n=\dim_K(\mathfrak{m}/\mathfrak{m}^2)$)，那么，我们有

$$\mathfrak{m}=(a_1,\cdots,a_n)+\mathfrak{m}\cdot\mathfrak{m}.$$

应用定理6.27(Nakayama 引理)，请注意 $\mathrm{rad}(S)=\mathfrak{m}$，立得

$$\mathfrak{m}=(a_1,\cdots,a_n).$$

反之，设 $\mathfrak{m}=(a_1,\cdots,a_n)$，那么，$\{\bar{a}_1,\cdots,\bar{a}_n\}$ 显然是 $\mathfrak{m}/\mathfrak{m}^2$ 的一个生成元集。综上所述，我们得到

$$\dim_K(\mathfrak{m}/\mathfrak{m}^2)=\mathfrak{m}\text{ 的最小生成元集的基数.}$$

定义6.20 设S是诺德局部环，$\mathfrak{m}$ 是它的极大理想，

$$S/\mathfrak{m}=K,$$

那么，

1) S **的嵌入维数**定义为 $\text{emb-dim}\,S=\dim_K(\mathfrak{m}/\mathfrak{m}^2)$；

2) 如果 $\dim S=\text{emb-dim}\,S$，则称S为一个**正则局部环**。令

$$\mathfrak{m}=(x_1,\cdots,x_d),$$

此处 $d=\dim S$，那么$\{x_1,\cdots,x_d\}$称为S的一个**正则参数系**。

论讨 1) 根据定理6.41，对任给的诺德局部环S，恒有

$$\text{emb-dim}\,S\geqslant\dim S.$$

2) 正则局部环相当于几何上的**平滑点**或**非奇异点**，非正规

局部环相当于**奇异点或非平滑点**。参见下面的例子。

例23 令 k 是代数封闭域，$R=k[x_1,\cdots,x_n]$。我们已经知道

$$n=\dim R=\sup\{l:\ l=\dim R_{\mathfrak{m}},\ \mathfrak{m}\text{ 是极大理想}\}.$$

根据希尔伯特零点定理，R 的极大理想 $\mathfrak{m}$ 皆形如

$$\mathfrak{m}=(x_1-a_1,\cdots,x_n-a_n),\qquad a_i\in k.$$

不难看出，在平移映射 $x_i\to x_i-a_i$ 作用下，所有的 $R_{\mathfrak{m}}$ 都是同构的。因此，对任给的极大理想 $\mathfrak{m}=(x_1-a_1,\cdots,x_n-a_n)$ 而言，我们恒有

$$\dim R_{\mathfrak{m}}=n.$$

自然，$\{x_1-a_1,\cdots,x_n-a_n\}$ 是 $R_{\mathfrak{m}}$ 的一个参数系，所以

$$\text{emb-dim}\, R_{\mathfrak{m}}=\dim R_{\mathfrak{m}}.$$

于是 $R_{\mathfrak{m}}$ 都是正则局部环。换句话说，n 维仿射空间 K^n 的点都是非奇异点。

例24 令 $R=\boldsymbol{C}[x,y]/(x^2-y^3)=\boldsymbol{C}[\bar{x},\bar{y}]$，$\mathfrak{m}=(\bar{x},\bar{y})$，$S=R_{\mathfrak{m}}$。显然，$R\supset\boldsymbol{C}[\bar{x}]$，$S\supset\boldsymbol{C}[\bar{x}]_{(\bar{x})}$，而且 S 对 $\boldsymbol{C}[\bar{x}]_{(\bar{x})}$ 是整数相关的，于是

$$\dim S=\dim \boldsymbol{C}[\bar{x}]_{(\bar{x})}=1.$$

另一方面，$\mathfrak{m}/\mathfrak{m}^2$ 是由 $\{x^*,y^*\}$ 生成的（x^*,y^* 是 $\bar{x},\bar{y}$ 在 $\mathfrak{m}S/\mathfrak{m}^2S$ 中的象）。读者自行证明

$$\text{emb-dim}\, S=\dim_C(\mathfrak{m}/\mathfrak{m}^2)=2\geqslant\dim S.$$

因此，S 是一个非正则局部环，这相应于 $(0,0)$ 是复数曲线 $x^2-y^3=0$ 的奇异点。▌

对于参数系，我们有如下的定理。

定理6.43 设 S 是诺德局部环，$\{x_1,\cdots,x_n\}$ 是它的一个参数系。那么，$\dim(S/(x_1,\cdots,x_d))=n-d$。

证明 令 $R=S/(x_1,\cdots,x_d)$。显然，$(\bar{x}_{d+1},\cdots,\bar{x}_n)$ 是 R 的一个定义理想。立得

$$\dim R\leqslant n-d.$$

反之，令 $\{\bar{y}_1,\cdots,\bar{y}_s\}$ 是 R 的一个参数系，显然，$(x_1,\cdots,x_d,y_1,$

$\cdots,y_s)$是R的一个定义理想。所以$d+s\geqslant n$，即得

$$\dim R\geqslant n-d. \quad \blacksquare$$

由于正则诺德局部环在代数学与几何学中的重要性，我们给出下面的定理。

定理6.44 设S是诺德局部环，$\dim S=n$，$\mathfrak{m}$是它的极大理想，$K=S/\mathfrak{m}$，$\hat{S}$是S对$\mathfrak{m}$的完备化环。那么，我们有

1) S是正则诺德局部环$\Longleftrightarrow G_{\mathfrak{m}}(S)$同构于$n$元多项式环$K[t_1,\cdots,t_n]$；

2) S是正则诺德局部环$\Longleftrightarrow \hat{S}$是正则诺德局部环。

证明 1) $\Longleftarrow$。显然，$\mathfrak{m}/\mathfrak{m}^2$相当于$t_1,\cdots,t_n$的一次齐次式的集合，所以

$$\dim_K(\mathfrak{m}/\mathfrak{m}^2)=n=\dim S.$$

$\Longrightarrow$。令$\mathfrak{m}=(x_1,\cdots,x_n)$。显然，

$$G_{\mathfrak{m}}(S)\approx K[\bar{x}_1,\cdots,\bar{x}_n],$$

其中$\bar{x}_i\in\mathfrak{m}/\mathfrak{m}^2$。我们仅须证明$\bar{x}_1,\cdots,\bar{x}_n$代数无关就足够了。设$\bar{f}\in K[X_1,\cdots,X_n]$，$\bar{f}\neq 0$，

$$G_{\mathfrak{m}}(S)\ni\bar{f}(\bar{x}_1,\cdots,\bar{x}_n)=\sum_i\bar{f}_i(\bar{x}_1,\cdots,\bar{x}_n)=0.$$

此处$\bar{f}_i$是i次齐次式。因为$\bar{x}_1,\cdots,\bar{x}_n$都是一次齐次式，$G_{\mathfrak{m}}(S)$是分次环，所以每一个$\bar{f}_i(\bar{x}_1,\cdots,\bar{x}_n)=0$。因此，不妨即设$\bar{f}$是一个$r$次齐次式。令

$$\sigma: K[X_1,\cdots,X_n]\to G_{\mathfrak{m}}(S),$$
$$\sigma(X_i)=\bar{x}_i.$$

再令$R=K[X_1,\cdots,X_n]/(\bar{f})=K[\bar{y}_1,\cdots,\bar{y}_n]$。又设

$$l_1(i)=\text{length}\{\bar{g}\in K[\bar{x}_1,\cdots,\bar{x}_n]:\deg\bar{g}<i\},$$
$$l_2(i)=\text{length}\{\bar{h}\in K[\bar{y}_1,\cdots,\bar{y}_n]:\deg\bar{h}<i\}.$$

我们要比较$l_1(i)$与$l_2(i)$。由于$\bar{f}\in\ker\sigma$，所以有

(a) $l_1(i)\leqslant l_2(i)$；

我们又有

(b) 当 i 充分大时，$l_1(i)(=\chi^S_{\mathfrak{m}}(i))$是 i 的多项式，且

$$\deg_i l_1(i)=\deg_x\chi^S_{\mathfrak{m}}(x)=\dim S=n。$$

（参看例19，请读者自证。）

(c) 当 i 充分大时，$l_2(i)$是 i 的多项式，且

$$\deg_i l_2(i)\leqslant n-1。$$

上面的(a),(b),(c)显然是矛盾的。

2) 根据定理6.39，我们知道 $\hat{S}$ 是诺德环。又有 $\hat{S}/\hat{\mathfrak{m}}\approx S/\mathfrak{m}$（为什么？），所以$\hat{\mathfrak{m}}$是$\hat{S}$的一个极大理想。任取 $\hat{a}\in\hat{\mathfrak{m}}$，那么

$$(1-\hat{a})^{-1}=1+\hat{a}+\cdots+\hat{a}^m+\cdots\in\hat{S},$$

所以 $1-\hat{a}$ 都是可逆元，于是

$$\hat{\mathfrak{m}}\subset\operatorname{rad}(\hat{S})=\bigcap_{\text{极大理想}}\mathfrak{p}_i。$$

由此即知$\hat{\mathfrak{m}}$是$\hat{S}$的唯一的极大理想，$\hat{S}$是一个局部环。因为

$$G_{\mathfrak{m}}(S)=\bigoplus_{i=0}^{\infty}(\mathfrak{m}^i/\mathfrak{m}^{i+1})\approx\bigoplus_{i=0}^{\infty}(\hat{\mathfrak{m}}^i/\hat{\mathfrak{m}}^{i+1})=G_{\hat{\mathfrak{m}}}(\hat{S}),$$

所以 $\dim S=\dim\hat{S}=n$，而且

$$G_{\mathfrak{m}}(S)\approx K[t_1,\cdots,t_n]\Longleftrightarrow G_{\hat{\mathfrak{m}}}(\hat{S})\approx K[t_1,\cdots,t_n]。\quad\blacksquare$$

下面这个定理的证明，要用到同调代数的方法，我们不加证明了。

定理6.45(Auslander-Buchsbaum 定理) 任何正则诺德局部环都是唯一分解整环。

证明请见 Zariski-Samuel 著《Commutative Algebra》，2卷，附录7，或 Matsumura 著《Commutative Algebra》，142页。

从这个定理，我们立刻看出，任何正则诺德局部环 S 都是整数封闭的等等，

我们很容适证明正则诺德局部环必定是一个整环。设 $a\neq 0$，$b\neq 0$，$ab=0$。令 $a\in\mathfrak{m}^{r_1}\backslash\mathfrak{m}^{r_1+1}$，$b\in\mathfrak{m}^{r_2}\backslash\mathfrak{m}^{r_2+1}$，则

$$\bar{a}\in \mathfrak{m}^{r_1}/\mathfrak{m}^{r_1+1},\quad \bar{a}\neq 0,$$
$$\bar{b}\in \mathfrak{m}^{r_2}/\mathfrak{m}^{r_2+1},\quad \bar{b}\neq 0,$$
但 $\bar{a}\bar{b}=0\in G_{\mathfrak{m}}(S)$。可是

$$G_{\mathfrak{m}}(S)=\oplus(\mathfrak{m}^i/\mathfrak{m}^{i+1})\approx K[t_1,\cdots,t_n].$$
这显然是不可能的。

我们又有下面的重要定理。

定理6.46(I.S.Cohen 定理) 设 $\hat{S}$ 对 $\hat{\mathfrak{m}}$ 是一个完备的诺德局部环。设 $\hat{S}$ 的特征等于 $\hat{S}/\hat{\mathfrak{m}}$ 的特征(所谓一个环 R 的特征数或特征，即是 $\min\{n: n\cdot 1=0,\ n$ 为正整数$\}$。如果 $n\cdot 1$ 永不为零，则称 R 的特征为 0)，那么

$$\hat{S}\approx K[[t_1,\cdots,t_n]].$$

证明请见 Zariski-Samual 著《Commutative Algebra》，2卷，304页。

讨论 当 $\hat{S}$ 含有一个域 k 时，上定理显然是对的。如果取 $S=\boldsymbol{Z}_{(p)}$，$\hat{S}=\hat{\boldsymbol{Z}}_{(p)}$，显然可见，上面的定理的假设是不可免去的。在一般的几何学中，$\hat{S}$ 都包含一个域，因此我们可以用它的结论。

习　　题

1. 令 $R=\boldsymbol{C}[[x,y,z]]/(x^2+xy+z^2)$。考虑 $(\bar{x},\bar{y}),(\bar{x},\bar{z}),(\bar{y},\bar{z})$，它们之中哪些是定义理想？哪些不是定义理想？其几何意义是什么？

2. 设 R 是正则局部环。证明 $\dim R=0\Longleftrightarrow R$ 是域。

3. 设 R 是诺德局部环，$\mathfrak{m}$ 是极大理想，$\hat{R}$ 是 R 在 $\mathfrak{m}$-adic 拓扑下的完备化环。证明 $\dim R=\dim\hat{R}$。

4. 设 R 是正则诺德局部环，$\mathfrak{m}$ 是它的极大理想，$\mathfrak{m}\neq(0)$。证明 $\mathfrak{m}\neq\mathfrak{m}^2$，取 $x\in\mathfrak{m}\backslash\mathfrak{m}^2$，证明 $R/(x)$ 是正则诺德局部环，且

$$\dim(R/(x))=\dim R-1.$$

5. 参考上题。更一般地，设 R 是诺德局部环，$\mathfrak{m}$ 是其极大理想。设 $x\in\mathfrak{m}$，x 不是零因子，证明

$$\dim(R/(x)) = \dim R - 1.$$

6. 设 $f(x_1, x_2, \cdots, x_n)$ 为 $C[x_1, x_2, \cdots, x_n]$ 中不可约多项式。证明：

$$P = (a_1, a_2, \cdots, a_n) \text{ 是 } f \text{ 的零点而 } \left.\frac{\partial f}{\partial x_i}\right|_P \text{ 不全为零}$$

$$\Longleftrightarrow (C[x_1, \cdots, x_n]/(f(x_1, \cdots, x_n)))_{(x_1 - a_1, \cdots, x_n - a_n)}$$

是正则诺德局部环。

7. 设 R 是环，$a_1, a_2, \cdots, a_n \in R$。如果

(1) $(a_1, a_2, \cdots, a_n) \neq R$，且

(2) a_i 不是 $R/(a_1, a_2, \cdots, a_{i-1})$ 的零因子 ($\forall i = 1, 2, \cdots, n$)，

则称 $\{a_1, a_2, \cdots, a_n\}$ 是一个 R 序列。设 K 是域，$R = K[x, y, z]$，$a_1 = x(y-1)$，$a_2 = y$，$a_3 = z(y-1)$，试证 $\{a_1, a_2, a_3\}$ 是 R 序列，而 $\{a_1, a_3, a_2\}$ 不是 R 序列。

8. 参考上题。设 R 是正则诺德局部环，$\mathfrak{m}$ 是它的极大理想。又设 $\dim R = n$，试证 $\mathfrak{m}$ 可以由一个 R 序列 $\{a_1, a_2, \cdots, a_n\}$ 生成。

9. 设 R 是诺德局部环，$\mathfrak{m}$ 是它的极大理想。又设 $\mathfrak{m}$ 可以由 R 序列生成，证明 R 必是正则局部环。

10. 不应用 Auslander-Buchsbaum 定理，直接证明正则诺德局部环是整数封闭的。

第七章 赋 值 论

§1 定 义

读者请参看第一章§6 "p-adic 数与赋值". 在本章我们将把那里的讨论充分地一般化. 我们先引入:

定义7.1 设G是一个加法交换群. 如果G含有一个半群G_+ (即$a,b\in G_+\Longrightarrow a+b\in G_+$), 使得$G=(-G_+)\cup\{0\}\cup G_+$, 而且这三个子集是两两不相交的, 那么, 称$G$为**加法交换全序群**, 或简称**全序群**. 我们用G_-表示$-G_+$. 此时, 我们有一个全序, 其定义如下:

$$a>b \Longleftrightarrow a-b\in G_+.$$

讨论 1) 读者用G_+是半群的性质, 检验

$$a>b,\ b>c \Longrightarrow a>c,$$

$$a>b,\ c>d \Longrightarrow a+c>b+d,$$

等等.

2) 反之, 设G有一个全序 ">", 适合上面的不等式, 那么, 令$G_+=\{a: a>0\}$, 读者自行检验G_+是一个半群; $-G_+$, $\{0\}$, G_+是两两不相交的, 及$G=(-G_+)\cup\{0\}\cup G_+$.

例1 $\boldsymbol{R}$的加法子群G都是全序群. 易见

$$G=(R_-\cap G)\cup\{0\}\cup(R_+\cap G)=G_-\cup\{0\}\cup G_+.$$

同样的, 任何一个全序群的子群, 也是全序群.

例2 在$G=\boldsymbol{Z}\oplus\boldsymbol{Z}$中, 我们可以定义一个**字母全序**:

$$G_+=\{(n_1,n_2):\ n_1>0 \text{ 或 } n_1=0,\ n_2>0\}.$$

换一个方式来说,

$$(n_1,n_2)>(m_1,m_2)\Longleftrightarrow(n_1-m_1,n_2-m_2)\in G_+$$

$$\Longleftrightarrow n_1>m_1 \text{ 或 } n_1=m_1,\ n_2>m_2.$$

这和查英文字典一样，先看头一个数字，如果两个元素有相同的首项，再看第二个数字。

与上面一样的，设 $G_1, \cdots, G_n$ 都是全序群。令 $G = \bigoplus_{i=1}^{n} G_i$，我们可以定义一个"字母全序"：

$$G_+ = \{(g_1, \cdots, g_n): 存在一个\ i\ ，使\quad g_i > 0,\ g_j = 0,\ \forall j < i\}.$$

现在我们引入赋值的定义。

定义7.2 设 K 是一个域，$K^* = K \backslash \{0\}$，G 是一个全序群。如果一个满射 $v: K^* \to G$，适合下列的条件，则称为 K 的一个**指数赋值**，或简称**赋值**：

1） $v(ab) = v(a) + v(b)$；

2） $v(a+b) \geqslant \min\{v(a), v(b)\}$。

讨论 1）以上的定义中，用的是加法全序交换群 G。同样，也可以用**乘法全序交换群** $G^* = G_1^{-1} \cup \{1\} \cup G_1$，这里 $G_1 = \{g: g < 1\}$ 是一个乘法半群，与加法全序交换群 G 中的加法半群 $G_+ = \{g: g > 0\}$ 相对应。赋值 v 的定义条件，也相应地改成：

1*） $v(ab) = v(a)v(b)$；

2*） $v(a+b) \leqslant \max\{v(a), v(b)\}$。

与下面的**三角不等式** 3*）相比，2*）称为**强三角不等式**：

3*） $v(a+b) \leqslant v(a) + v(b)$。

不过，除了特别声明外，一般我们都用加法全序交换群，而不用乘法全序交换群。

2）从定义7.2的条件 1），我们导出

$$v(b) = v(1 \cdot b) = v(1) + v(b) \Longrightarrow v(1) = 0,$$

$$0 = v(1) = v(b \cdot b^{-1}) = v(b) + v(b^{-1})$$

$$\Longrightarrow v(b^{-1}) = -v(b),$$

$$v(ab^{-1}) = v(a) + v(b^{-1}) = v(a) - v(b).$$

所以，v 是从乘法群 K^* 到加法群 G 的一个群映射。

例3 1）第一章§6中$\boldsymbol{Q}$的p赋值v_p是用乘法全序交换群$G^*=\{p^i: i\in \boldsymbol{Z}\}$定义的赋值。

2）令K为复变函数论的“在$x=0$附近的亚纯函数域”，即$\boldsymbol{C}\{\{x\}\}$（参见第六章§8）的比域。令$G=\boldsymbol{Z}$。以$v_x(f)$表示f的阶，即设

$$f=\sum_{i=m}^{\infty}a_m x^i,\quad a_m\neq 0,\ m\in \boldsymbol{Z},$$

那么$v_x(f)=m$。读者自行检验，v_x确实是一个赋值。

3）令R是一个唯一分解的整环，a是一个不可分解元，K是R的比域，$G=\boldsymbol{Z}$。任取

$$\frac{c}{b}a^n\in K,\quad a\nmid b,\ a\nmid c,\ n\in \boldsymbol{Z},$$

我们定义

$$v_a\left(\frac{c}{b}a^n\right)=n.$$

读者自行检验，v_a是一个赋值。

特别是当$R=\boldsymbol{C}[x]$，那么，$a=c_0x-c_1$（$c_0\neq 0$）。v_a是一个赋值。

4）令$K=\boldsymbol{C}(x,y)$，$G=\boldsymbol{Z}\oplus\boldsymbol{Z}\sqrt{2}$。按照例2的讨论，$G$自然是一个全序群。令

$$v(f(x,y))=\mathrm{ord}_t f(t,t^{\sqrt{2}}),$$

其中ord_t表示t的阶。则v是一个赋值。

5）我们可以把v扩充到整个K。定义$v(0)=\infty$，其中的无限大“∞”，适合下列条件：

$$\infty>g,\quad \forall g\in G,$$

$$\infty\pm g=\infty,\quad \infty+\infty=\infty,\quad \infty-\infty\text{没有定义。}$$

那么，对于任意的$a,b\in K$，我们恒有

$$v(ab)=v(a)+v(b),\quad v(a+b)\geqslant \min\{v(a),v(b)\},$$

定义7.3 设K是域，R是K的子环．如果对于任取的$a\in K$，$a\neq 0$而言，a, a^{-1}二者之中至少有一个在R中，那么，R称为K的一个**赋值环**．

讨论 R的比域显然是K．

定理7.1 1）设R是域K的子环，K是R的比域．那么，R是K的赋值环$\Longrightarrow \mathfrak{m}=\{a: a$是$R$的不可逆元$\}$是$R$的唯一的极大理想，所以$R$是局部环．

2）设v是K的赋值．令

$$R_v=\{a: a\in K,\ v(a)\geqslant 0\}.$$

那么，R_v是K的一个赋值环．

证明 1）显然，ab是可逆元$\Longrightarrow a$及b是可逆元，所以

$$b\in\mathfrak{m} \Longrightarrow ab\in\mathfrak{m},\qquad \forall a\in R.$$

仅须证明$a,b\in\mathfrak{m}\Longrightarrow a+b\in\mathfrak{m}$，便知$\mathfrak{m}$是一个理想．

考虑a/b及b/a，二者之一必在R中．无妨假定$a/b\in R$．于是

$$1+(a/b)=(a+b)/b\in R.$$

假若$a+b$是可逆元，那么$1/b\in R$，即b是可逆元，这与已知条件相违．所以$a+b\in\mathfrak{m}$，$\mathfrak{m}$是一个理想，且显然是唯一的极大理想．

2）设$a\bar{\in} R_v$，则$v(a)<0$．于是

$$v(a^{-1})=-v(a)>0 \Longrightarrow a^{-1}\in R_v. \quad \blacksquare$$

定理7.1说明了，给定一个赋值v以后，我们自然得出一个赋值环R_v．反过来说，给定一个赋值环R以后，能不能自然地得出一个赋值呢？这是能作到的．作法如下（这里我们用乘法全序交换群）．

令$\mathfrak{m}$是R的极大理想，$\mathfrak{m}^*=\mathfrak{m}\backslash\{0\}$，$U$是$R$的所有可逆元的集合，即$U=R\backslash\mathfrak{m}$．如果$a\bar{\in} R$，那么$a^{-1}\in R$，但$a^{-1}\bar{\in} U$，所以$a^{-1}\in\mathfrak{m}$，$a\in(\mathfrak{m}^*)^{-1}$，也即

$$K^*=K\backslash\{0\}=(\mathfrak{m}^*)^{-1}\cup U\cup\mathfrak{m}^*.$$

这是一个乘法交换群，U是它的正规子群，所以

$$K^*/U=((\mathfrak{m}^*)^{-1}/U)\cup\{1\}\cup(\mathfrak{m}^*/U)=G_1^{-1}\cup\{1\}\cup G_1,$$

这就给出 K^*/U 的一个全序。令 U: $K^*\to K^*/U$ 为典型映射，那么显然有（参见定义7.2的讨论 1））

$$v(ab)=v(a)v(b).$$

任取 $a,b\in K^*$，设 $a/b\in R$，那么

$$v(a+b)=v\left(b\left(1+\frac{a}{b}\right)\right)=v(b)v\left(1+\frac{a}{b}\right)\leqslant v(b)$$

$$\leqslant\max\{v(a),v(b)\}.$$

所以验证了强三角不等式 2*)。因此，v 是一个赋值。

以上由赋值环R定义的赋值 v，称为赋值环R的**典型赋值**。

定义7.4 两个赋值 v_1,v_2，如果它们的赋值环相等，那么，我们称 v_1,v_2 是**等价的**。

给定了K的一个赋值环R以后，我们可以定义一个映射

$$\sigma:\ K\to(R/\mathfrak{m})\cup\{\infty\}$$

如下：

$$\sigma:\ R\to R/\mathfrak{m}\text{是典型映射},$$

$$\sigma(a)=\infty,\ \text{如果}a\overline{\in}R.$$

这个 σ 就是通常所说的“位”。

定义7.5 域K的一个**位**是指一个映射 σ: $K\to L\cup\{\infty\}$，此处L是域，σ 适合下列条件：

1） $\sigma^{-1}(L)$是K的子环，σ: $\sigma^{-1}(L)\to L$ 是环映射；

2） 如果 $a\in\sigma^{-1}(\infty)$，那么 $\sigma(a^{-1})=0$。

讨论 从上面的定义不难看出，在 $L\cup\{\infty\}$中

$$l\pm\infty=l\cdot\infty=\infty,\quad l\in L^*=L\backslash\{0\},$$

$$\infty\cdot\infty=\infty,\quad \frac{1}{0}=\infty,\quad \frac{1}{\infty}=0,$$

$$\infty\pm\infty,\quad 0\cdot\infty,\quad \frac{0}{0},\frac{\infty}{\infty}\text{无定义。}$$

例4 设$K=\boldsymbol{C}(x)$，$L=\boldsymbol{C}$，$R=\boldsymbol{C}[x]_{(x-a)}$，$v(f)=\mathrm{ord}_{(x-a)}f(x)$，$\sigma(f)=f(a)$。$\sigma(f)$即是$f(x)$在"位"$x=a$的值。如果$\sigma(f)=f(a)=\infty$，那么，$f(x)$在位$a$有一个极点。▎

上面我们已经说明了，给了一个赋值环R以后，自然得出一个位σ。反之，给定了一个位σ，令$R=\sigma^{-1}(L)$，根据条件2)，$a\bar{\in}R(\Longleftrightarrow a\in\sigma^{-1}(\infty))\Longrightarrow\sigma(a^{-1})=0\in L\Longrightarrow a^{-1}\in\sigma^{-1}(L)\Longrightarrow a^{-1}\in R$，所以，我们自然得出一个赋值环$R$。

综上所述，这三个概念：赋值v，赋值环R，位σ，是自然对应的。因此，从更高的抽象层次来看，这三者是完全一样的。

定理7.2 1) 设$v(a)<v(b)$，那么$v(a+b)=v(a)$；

2) 设$v(a_1+\cdots+a_n)=\infty$，即$a_1+\cdots+a_n=0$，那么，至少有两个a_i,a_j，使$v(a_i)=v(a_j)=\min\{v(a_l):\ l=1,\cdots,n\}$；

3) 设I是赋值环R的有限生成的理想，那么I是主理想。

证明 1) $v(b/a)=v(b)-v(a)>0\Longrightarrow b/a\in\mathrm{m}\subset R_v\Longrightarrow 1+b/a\bar{\in}\mathrm{m}\Longrightarrow v(1+b/a)=v((a+b)/a)=0\Longrightarrow v(a+b)=v(a)$。

2) 不难从1)导出。假如$v(a_1)<v(a_l)(\forall l=2,3,\cdots,n)$，则有

$$v(a_1+a_2)=v(a_1)<v(a_3),$$
$$v(a_1+a_2+a_3)=v(a_1+a_2)=v(a_1)<v(a_4),$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$v(a_1+a_2+\cdots+a_n)=v(a_1).$$

3) 设$I=(a_1,a_2)$，$v(a_1)\leqslant v(a_2)$。那么$v(a_2/a_1)\geqslant 0$，故

$$a_2/a_1\in R_v,\qquad a_2=(a_2/a_1)a_1\in(a_1).$$

所以$I=(a_1)$。不难推广到I是有限生成的理想的情形。▎

定理7.3 1) 如果赋值环R是诺德环，那么$\dim R\leqslant 1$。此时只有两种可能：$\dim R=0\Longrightarrow R=K$；$\dim R=1\Longrightarrow R$是正则诺德局部环。

2) R 是一维的正则诺德局部环$\Longleftrightarrow R$ 是整环，且是它的比域K的赋值环，相应的全序群 $G\approx \boldsymbol{Z}$。

证明 1) 因为R的极大理想 m 是有限生成的，应用上定理，$\mathfrak{m}=(a)$。根据定理6.41，立得

$$\dim R\leqslant 1.$$

当 $\dim R=0$ 时，因为R是整环，所以(0)是R的素理想，因而是极大理想。假若有 $b\in K$，$b\overline{\in} R$，那么 $b^{-1}\in(0)$。这是不可能的。所以 $R=K$。当 $\dim R=1$ 时，上面所说的 m 的生成元集$\{a\}$就是R的正则参数系，所以R是正则局部环。

2) $\Longrightarrow$。根据定理 6.46 前面的讨论，我们知道R是整环。令它的比域为K，极大理想为 $\mathfrak{m}=(a)$。任取 $b\in R$，$b\neq 0$，设

$$b\in \mathfrak{m}^l,\ b\overline{\in}\mathfrak{m}^{l+1},\quad l\in \boldsymbol{Z},$$

即 $b=a^lc$，$c\in R\backslash\mathfrak{m}$。那么，$c$ 是可逆元。现考虑任意的 $b_1/b_2\in K(b_2\neq 0)$。令

$$b_1=a^{l_1}c_1,\ b_2=a^{l_2}c_2,\quad c_1,c_2\in R\backslash\mathfrak{m}.$$

那么，

$$l_1\geqslant l_2 \Longrightarrow b_1/b_2=a^{l_1-l_2}c_1/c_2\in R.$$

所以R是K的赋值环。显然，

$$v(b)=l,\quad v(0)=\infty$$

是K的一个赋值，且$R_v=R$。其相应的全序群是 $\boldsymbol{Z}$。

$\Longleftarrow$。设 $t\in R$，使得 $v(t)=1\in G=\boldsymbol{Z}$。任取 $a\in R$，设$v(a)=l$。令 $b=a/t^l$，即 $a=bt^l$，则 $v(b)=0$，即 b 是可逆元。所以

$$\mathfrak{m}=\{a\in R:\ v(a)>0\}=\{bt^l\in R,\ l\geqslant 1,\ b\text{ 可逆}\}=(t).$$

现设 I 是R的理想，不难看出 $I=(a)$，此处 a 满足

$$v(a)=\min\{v(c):\ c\in I\}.$$

于是 $I=(t^l)$。立得(0)及 m 是R仅有的素理想。故 $\dim R=1$，$\{t\}$是正则参数系。所以R是一维正则局部环。 ▎

定义7.6 如果一个赋值 v 的全序群 $G\approx\boldsymbol{Z}$，那么，称 R_v为**（一秩）离散赋值环**，简称 D.V.R.。

当赋值 v 的赋值环 $R_v=K$ 时，不难看出，v 的全序群 $G=\{0\}$。此时，称 v 是一个**平凡赋值**。

我们举出下面的例子，说明赋值的全序群可以是任意的。

例 5 设 G 是任给的加法交换全序群，k 是任给的域。令

$$S=\{a_1x^{g_1}+\cdots+a_nx^{g_n}:\ a_i\in k,\ g_i\in G,\ n\text{是非负整数},\ x^0=1\}.$$

定义

$$ax^g+bx^g=(a+b)x^g,\qquad ax^{g_1}\cdot bx^{g_2}=abx^{g_1+g_2},$$

则S自然成一整环(为什么？)。令 K 是 S 的比域。定义

$$v(\sum a_ix^{g_i})=\min\{g_i:\ a_i\neq 0\},$$

$$v\left(\frac{\sum a_ix^{g_i}}{\sum b_jx^{g_j}}\right)=v(\sum a_ix^{g_i})-v(\sum b_jx^{g_j}).$$

那么，v 是 K 的一个赋值，而 G 是它的全序群。▌

根据定理 7.3，一般来说，一个赋值环 R 不一定是诺德环。它有很多与诺德环不一样的性质。请看下面的定理。

定理7.4 1) 设 R 是赋值环，K 是其比域。设有环 S，$K\supset S\supset R$，那么，S 是一个赋值环。设 $\mathfrak{n}$ 是 S 的极大理想，$\mathfrak{p}=\mathfrak{n}\cap R$，则有 $S=R_{\mathfrak{p}}$；

2) 设 I_1,I_2 是 R 的两个理想，那么，必有 $I_1\subset I_2$ 或 $I_2\subset I_1$。

证明 1) 任取 $a\in K$，$a\neq 0$，那么必有 a 或 $a^{-1}\in R\subset S$。所以，S 是一个赋值环。令 $\mathfrak{n}$ 是 S 的极大理想，$\mathfrak{p}=\mathfrak{n}\cap R$，$\mathfrak{p}$ 显然是 R 的一个素理想。我们要证明$S=R_{\mathfrak{p}}$。

任取 $a=c/b\in R_{\mathfrak{p}}$，$c,b\in R$，$b\notin\mathfrak{p}$。那么 $b\in S$，$b\notin\mathfrak{n}$。所以 b 在 S 中是可逆元。于是 $a\in S$。我们证明了$R_{\mathfrak{p}}\subset S$。

反之，设 $a\in S$。如果 $a\in R$，则$a\in R_{\mathfrak{p}}$。如果$a\notin R$，那么$a^{-1}\in R\subset S$。于是$a,a^{-1}\in S$，即 a 是 S 的可逆元，所以 $a,a^{-1}\notin\mathfrak{n}\Longrightarrow a^{-1}\notin\mathfrak{n}\cap R=\mathfrak{p}\Longrightarrow a=1/a^{-1}\in R_{\mathfrak{p}}$。我们证明了 $S\subset R_{\mathfrak{p}}$。于是$S=R_{\mathfrak{p}}$。

2) 设 $I_1 \not\subset I_2$。任取 $a \in I_1 \backslash I_2$，$b \in I_2$。因为 $(a/b)b = a$，所以 $a/b \notin R$。故 $b/a \in R$，$b = (b/a)a \in aR \subset I_1$。 ▎

定义7.7 设 R 是一个赋值环。根据上面的定理，R 的素真理想 $\mathfrak{p}_i$(即 $\mathfrak{p}_i \neq R, (0)$) 对于"$\subset$"而言构成一个全序集。它的序数称为 R **的秩**，记为 rank R。显然，当 rank R 是有限数时，

$$\text{rank } R = \dim R.$$

讨论 1) 在代数数论中，我们对一秩的赋值有兴趣。在代数几何学中，我们对有限秩的赋值有兴趣，特别是一秩的赋值。详见后面。

2) 我们也可以用一个赋值 v 的全序群 G，来定义 v 的秩。G 的一个子群 H，如适合下列的条件，则称为 G 的一个**孤立子群**：(a) 任取 $h \in H$，那么，只要 $-h \leqslant g \leqslant h$，则 $g \in H$；(b) H 是 G 的真子群 (即 $H \neq G$)。我们可以证明：(a) G 的所有孤立子群的集合，对"$\supset$"而言构成一个全序集；(b) 令 $\mathfrak{p}$ 是 R_v 的一个素理想，那么

$$\mathfrak{p} \mapsto G_{\mathfrak{p}} = G \backslash (v(\mathfrak{p}^*) \cup v((\mathfrak{p}^*)^{-1}))$$

(这里 $\mathfrak{p}^* = \mathfrak{p} \backslash \{0\}$)是从 R_v 的素真理想的集合到 G 的孤立子群的集合的单满映射，而且保持序关系。因此，两者的序数是相同的。因而，我们又有下面的定义。

定义7.7′ v 的秩定义为 G 的孤立子群的序数。

例6 设 $\{0\} \neq G \subset \boldsymbol{R}$，我们称这样的赋值 v 为**实赋值**。此时，G 的唯一的孤立子群是 $\{0\}$(为什么？)，所以 rank $R_v = 1$。我们也可以从定义 7.7 直接导出 $\text{rank}(R_v) = 1$：令 R_v 的极大理想是 $\mathfrak{m}_v$。任取 R_v 的真理想 $I \neq (0)$，我们只要证明 $\sqrt{I} = \mathfrak{m}_v$ 就足够了(因为此时 (0) 与 $\mathfrak{m}_v$ 是 R_v 的仅有的素理想，所以，$1 = \dim R_v = \text{rank } R_v$)。令 $0 \neq a \in I$，任取 $b \in \mathfrak{m}_v$，$b \neq 0$。那么，对足够大的 n，我们有

$$v(b^n) = nv(b) > v(a),$$

即 $b^n/a \in R_v$，$b^n = (b^n/a)a \in I$，即有 $\sqrt{I} = \mathfrak{m}_v$。反过来说，只

要G的唯一的孤立子群是$\{0\}$，那么，经过一些初等数论的、类似于 Dedekind 分割的步骤，我们可以把G嵌入$\boldsymbol{R}$。综上所述，我们知道实赋值即是一秩赋值。

例7 设v是域K的一个一秩赋值，也即是一个实赋值。那么，我们可以定义一个绝对值"$|\ |_v$"如下：设$a\in K$，则

$$|a|_v=2^{-v(a)}, \qquad |0|_v=2^{-\infty}=0。$$

这也就是把加法交换全序群G变成了一个乘法交换全序群$G^*\subset \boldsymbol{R}_+$（$\boldsymbol{R}_+$表示全体正实数构成的乘法群）。这个绝对值适合（参见定义7.2的讨论 1））：

1*) $|ab|_v=|a|_v|b|_v$；

2*) $|a+b|_v\leqslant\max\{|a|_v,|b_v|\}$。

此时，域K称为一个**赋值域**。对于这样的域K，我们可以引入解析函数论及解析几何学。先定义n元解析函数环，或n元收敛函数环$K\{\{x_1,\cdots,x_n\}\}$如下（参见第六章§2）：

$$K\{\{x_1,\cdots,x_n\}\}=\left\{\sum f_{i_1\cdots i_n}x_1^{i_1}\cdots x_n^{i_n}: \text{存在}A\text{及}B\in\boldsymbol{R}\text{，使}\ |f_{i_1\cdots i_n}|_v\leqslant AB^{i_1+\cdots+i_n}\right\}.$$

显然$K\{\{x_1,\cdots,x_n\}\}\subset K[[x_1,\cdots,x_n]]$.经过它的谱集$\mathrm{Spec}K\{\{x_1,\cdots,x_n\}\}$（见第六章），我们可以建立相应的解析几何学。

定义7.8 1）设R_v是v的赋值环。如果$R_v\supset k$，此处k是一个域。那么v也称为k**赋值**；

2）设v是k赋值。那么，它对k的**剩余维数** $\text{res-dim}_k v$ 定义为 $\text{res-dim}_k v=\operatorname{tr}\deg((R_v/\mathrm{m}_v)/k)$。如果 $\text{res-dim}_k v=0$，则称v是**剩余代数性的**，如果$R_v/\mathrm{m}_v=k$，则称v是**剩余有理性的**。

引理 1）设$\bar{k}$是k在K里的代数闭包，那么，任何一个k赋值v，必定是$\bar{k}$赋值；

2）设k赋值v不是平凡的，$\operatorname{tr}\deg(K/k)=n<\infty$，那么

$$\text{res-dim}_k v\leqslant n-1.$$

证明 1）任取$0\neq a\in\bar{k}$，适合下面的方程式

$$a^l + b_1 a^{l-1} + \cdots + b_l = 0, \qquad b_i \in k.$$

应用定理7.2，必有 $0 \leqslant j < i \leqslant l$，使

$$v(b_i a^{l-i}) = v(b_j a^{l-j}),$$

故
$$v(a^{i-j}) = v(b_i) - v(b_j) = 0 - 0 = 0.$$

所以 $v(a) = 0$，$a \in R_v$。

2) 由于 v 不是平凡的，所以 $\mathfrak{m}_v \neq (0)$。任取 $x \in \mathfrak{m}_v \setminus \{0\}$。根据 1)，即知 $x \overline{\in} \bar{k}$(因为 $\bar{k} \setminus \{0\}$的元素都是可逆元)。所以 x 对 k 是超越的。而在典型映射 σ: $R_v \to R_v/\mathfrak{m}_v$ 之下，$\sigma(x) = 0$，所以

$$\text{res-dim}_k v \leqslant n - 1. \quad \blacksquare$$

下面的定理给出了 $\operatorname{rank} v (= \operatorname{rank} R_v)$ 与 $\text{res-dim}\, v$ 之间的关系。

定理7.5 设 v 是 k 赋值，K 对 k 的超越次数

$$\operatorname{tr\,deg}(K/k) = n < \infty.$$

那么
$$\operatorname{rank} v + \text{res-dim}\, v \leqslant n.$$

证明 设 $L_1 \supsetneqq L_2$ 是 K 的两个 k 赋值环。$\mathfrak{m}_1, \mathfrak{m}_2$ 是它们的极大理想。又设 $\mathfrak{p} = \mathfrak{m}_1 \cap L_2$。根据定理7.4，

$$L_1 = (L_2)_\mathfrak{p}, \qquad \mathfrak{m}_1 = \mathfrak{p}(L_2)_\mathfrak{p},$$

所以$L_1/\mathfrak{m}_1 = (L_2)_\mathfrak{p}/\mathfrak{p}(L_2)_\mathfrak{p} \supset L_2/\mathfrak{p}L_2$。令$\bar{K} = L_1/\mathfrak{m}_1$，$\bar{L}_2 = L_2/\mathfrak{p}L_2$，不难看出$\bar{K} \supset k$，$\bar{L}_2$ 是 $\bar{K}$ 的 k 赋值环，它的极大理想 $\mathfrak{m}_2/\mathfrak{p} \neq (0)$（否则 $L_2 = (L_2)_\mathfrak{p} = L_1$，矛盾），所以不是平凡的。显然

$$\text{res-dim}\, L_2 = \text{res-dim}\, \bar{L}_2, \quad \operatorname{tr\,deg}(\bar{K}/k) = \text{res-dim}\, L_1.$$

根据上面的引理，我们得出

$$\text{res-dim}\, L_2 < \text{res-dim}\, L_1.$$

回到本定理。设 $\operatorname{rank} v = \dim R_v = r$，则存在 R_v 的素理想链

$$(0) \subsetneqq \mathfrak{p}_1 \subsetneqq \cdots \subsetneqq \mathfrak{p}_r = \mathfrak{m}_v.$$

令 $L_i = (R_v)_{\mathfrak{p}_i}$，则

$$L_1 \supsetneqq \cdots \supsetneqq L_r = R_v.$$

故

$$n = \operatorname{tr}\deg(K/k) > \text{res-dim}\, L_1 > \cdots > \text{res-dim}\, L_r = \text{res-dim}\, R_v.$$

立得 $\quad n \geqslant r + \text{res-dim}\, R_v = \text{res-dim}\, v + \operatorname{rank} v.$

（我们常把 v 与 R_v 等同起来，就像在上面证明中把 $\operatorname{rank} R_v$ 记为 $\operatorname{rank} v$，把 $\text{res-dim}\, v$ 记为 $\text{res-dim}\, R_v$ 一样。）▮

例8 参见例 3 的 4)。设 $K = \boldsymbol{C}(x,y)$，$G = \boldsymbol{Z} + \boldsymbol{Z}\sqrt{2}$，

$$v(f(x,y)) = \operatorname{ord}_t f(t, t^{\sqrt{2}}).$$

那么，$\operatorname{tr}\deg(K/\boldsymbol{C}) = 2$，$\text{res-dim}\, v = 0$，$\operatorname{rank} v = 1$。所以

$$\operatorname{tr}\deg(K/\boldsymbol{C}) > \text{res-dim}\, v + \operatorname{rank} v.$$

习　题

1．写出 $\boldsymbol{Q}$ 的所有赋值。

2．设 K 是域，找出 $K(x)$ 的所有赋值 v，使 $\forall a \in K$，$v(a) = 0$。

3．设 R 是唯一分解整环，p 是素元，证明 $R_{(p)}$ 是赋值环。

4．设 v_p 表示 $\boldsymbol{Q}$ 内的 p-adic 赋值。在域 $K = \boldsymbol{Q}(\sqrt{5})$ 内，对 $5k \pm 2$ 型素数 p 及 $\alpha = a + b\sqrt{5} \neq 0$ $(a, b \in \boldsymbol{Q})$，定义

$$v(\alpha) = \frac{1}{2} v_p(a^2 - 5b^2).$$

证明 v 是 K 内的一个赋值。

5．试找出一个整环 R 及其中一个分母系 D，使 R_D 不是 R 的比域 K 的赋值环。

6．令 $K = \boldsymbol{C}(x_1, \cdots, x_n)$，又设 $a_1, \cdots, a_n \in \boldsymbol{R}$，在 $\boldsymbol{Q}$ 上线性无关。作变换 $x_i \mapsto t^{a_i}$，对 $f(x_1, \cdots, x_n) \in \boldsymbol{C}[x_1, \cdots, x_n]$，有

$$f(x_1, \cdots, x_n) \mapsto f(t^{a_1}, \cdots, t^{a_n}).$$

令 $v(f) = \operatorname{ord} f(t^{a_1}, \cdots, t^{a_n})$。对 $f, g \in \boldsymbol{C}[x_1, \cdots, x_n]$，令

$$v\left(\frac{f}{g}\right) = v(f) - v(g).$$

证明 v 是 K 的一个赋值，并求 rank v。

7．令 $K=\boldsymbol{C}(x_1,\cdots,x_n)$，对 $f(x_1,\cdots,x_n)\in\boldsymbol{C}[x_1,\cdots,x_n]$，定义

$$v(f)=f(x_1,\cdots,x_n)\text{中最低次项的次数。}$$

又令 $v(f/g)=v(f)-v(g)$。证明 v 是 K 的一个赋值，试求rank v 及 v 的赋值环。

8．设 R 是一个局部主理想整环，证明 R 是它的比域 K 的一个赋值环，且对应的赋值是离散赋值。

9．设 v 是域 K 的赋值，任取 $f(x)=\sum_{i=0}^{n}a_ix^{n-i}\in K[x]$，定义

$$v(f)=\min_i\{v(a_i)\}.$$

又令 $v(f/g)=v(f)-v(g)$。问 v 是否为域 $K(x)$ 的赋值？

10．续上题。设 v 是实赋值。我们定义

$$v(f)=\min_{0<i<n}\{v(a_i)/i\}.$$

又令 $v(f/g)=v(f)-v(g)$，问 v 是否为 $K(x)$ 的赋值？

11．证明赋值 v 是一秩的 $\Longleftrightarrow$ v 的全序群 G 有阿基米得性质，即任给 $a,b\in G$，$a>0$，那么存在 n，使 $na>b$。

12．设 $f(x,y)\in\boldsymbol{C}[x,y]$，不可约。又设 $(a_1,a_2)\in\boldsymbol{C}^2$，使得

$$f(a_1,a_2)=0,$$

但 $\frac{\partial f}{\partial x},\frac{\partial f}{\partial y}$ 在点 (a_1,a_2) 不全为0，令

$$R=\boldsymbol{C}[x,y]/(f(x,y))=\boldsymbol{C}[\bar{x},\bar{y}].$$

又设 $\mathfrak{m}=(\bar{x}-a_1,\bar{y}-a_2)$ 为 R 的一个极大理想，证明 $R_{\mathfrak{m}}$ 是 R 的比域 K 的一个赋值环，且对应的赋值是离散赋值。

13．设 R 是整环但不是域，证明下列命题等价：

(1) R 是局部诺德环，其极大理想是主理想；

(2) 存在一个素元 $t\in R$，使 R 内每个非零元素 x 可以唯一地表示成 $x=ut^n$，其中 u 为可逆元而 n 是非负整数。

§2 赋值的存在及扩充

设已给一域 K，v 是它的一个赋值，赋值环为 R_v，极大理想为 $\mathfrak{m}_v$。又设 S 是 K 的一个子环。当 $R_v\supset S$ 时，我们称 v 在 S 上是**有限的**。例如，$K=\boldsymbol{C}(x)$，$S=\boldsymbol{C}[x]$。任何一个

$$R_v=\boldsymbol{C}[x]_{(x-a)}\quad (a\in\boldsymbol{C})$$

在 S 上都是有限的。另有一个

$$R_v=\boldsymbol{C}[x^{-1}]_{(x^{-1})}$$

在 S 上是**无限的**。当 $R_v\supset S$ 时，$\mathfrak{m}_v\cap S=\mathfrak{p}$ 是 S 的素理想，称为 v 在 S 上的**中心**。例如，在上面的例子中，$\boldsymbol{C}[x]_{(x-a)}$ 的中心即是 $(x-a)$，相应于几何上的点 $x=a$。而 $\boldsymbol{C}[x^{-1}]_{(x^{-1})}$ 相应于无穷远点 $x=\infty$。它在 $\boldsymbol{C}[x]$ 上是无限的，也没有中心。

如果 S 是一个局部环，$\mathfrak{m}$ 是它的极大理想，那么是否存在一个赋值环 R_v，使 v 在 S 上是有限的，而且 v 在 S 的中心即是 $\mathfrak{m}$ 呢？我们将证明确实存在这样一个 v。

引理 设 S 是域 K 的子环，I 是 S 的真理想。任取 $0\neq a\in K$，那么，$IS[a]$ 是 $S[a]$ 的真理想，或者 $IS[a^{-1}]$ 是 $S[a^{-1}]$ 的真理想。

证明 假设 $IS[a]=S[a]$，且 $IS[a^{-1}]=S[a^{-1}]$，我们要导出一个矛盾。我们有下面二式

$$(1)\qquad 1=\sum_{i=0}^{n} b_i a^i,\qquad b_i\in I,$$

$$(2)\qquad 1=\sum_{j=0}^{l} c_j a^{-j},\qquad c_j\in I.$$

令 n,l 为满足(1),(2)二式的最小的正整数，不妨又设 $n\geqslant l$。由(2)式又得

(3) $$(1-c_0)a^n = \sum_{j=1}^{l} c_j a^{n-j}.$$

将(1)式乘以$(1-c_0)$后，以(3)式代入其右端最高次项，有

$$1-c_0=(1-c_0)\sum_{i=0}^{n-1} b_i a^i + b_n \sum_{j=1}^{l} c_j a^{n-j}.$$

将此式左端的c_0移至右端并整理，则得到一个系数均在I中但次数小于n的a的多项式，这与n的选取相矛盾。▎

定理7.6(存在定理) 1) 设S是域K的子环，I是S的理想，$I \neq S$。那么，存在K的一个赋值v，使

$$R_v \supset S, \quad \mathfrak{m}_v \cap S \supset I;$$

2) 更进一步，设S是局部环，$\mathfrak{m}$是它的极大理想。那么，存在K的一个赋值v，使$R_v \supset S$，$\mathfrak{m}_v \cap S=\mathfrak{m}$，即$v$在$S$的中心是$\mathfrak{m}$。

证明 1) 应用 Zorn 引理。令

$$\mathscr{F}=\{R:\ R\text{是}K\text{的子环},\ R\supset S,\ IR\neq R\}.$$

显然$S\in\mathscr{F}$，所以$\mathscr{F}\neq\varnothing$。包含关系"$\supset$"给出$\mathscr{F}$的一个半序。设$\{R_\alpha\}$是$\mathscr{F}$的一个链（即全序子集）。令$R^*=\bigcup R_\alpha$。我们要说明$R^*\in\mathscr{F}$。假设$IR^*=R^*$，那么有

$$1=\sum_{i=1}^{l} a_i b_i,\qquad a_i\in I,\ b_i\in R^*=\bigcup R_\alpha.$$

于是，存在一个α，使$b_i\in R_\alpha(\forall i=1,\cdots,l)$。立得$IR_\alpha=R_\alpha$，与$R_\alpha\in\mathscr{F}$相违。所以$IR^*\neq R^*$，即$R^*\in\mathscr{F}$。因此，$\mathscr{F}$适合 Zorn引理的条件。

令R是$\mathscr{F}$的一个极大元。我们要证明R是一个赋值环。任取$0\neq a\in K$，应用上面的引理，$IR[a]\neq R[a]$或$IR[a^{-1}]\neq R[a^{-1}]$。因此，$R[a]\in\mathscr{F}$或$R[a^{-1}]\in\mathscr{F}$。但已经知道R是$\mathscr{F}$的极大元，立得$R[a]=R$或$R[a^{-1}]=R$，即$a\in R$或$a^{-1}\in R$。

2) 由于$1\notin\mathfrak{m}_v$，所以$\mathfrak{m}_v\cap S\neq S$。于是必有$\mathfrak{m}_v\cap S=\mathfrak{m}$。▎

系1 设S是一个整环，但不是域，又设域$K\supset S$，那么存

在K的一个非平凡的赋值v，使得v在S上是有限的，即$R_v \supset S$。

证明 取S的一个非零素理想$\mathfrak{p}$。在上定理的1)中令$I=\mathfrak{p}$即可。 ▎

系 2 一个域K只有平凡赋值$\Longleftrightarrow K$是素域$\boldsymbol{Z}/p\boldsymbol{Z}$的代数扩域。

证明 $\Longrightarrow$。假若K的特征是0，则$K\supset \boldsymbol{Z}$。应用系1，令$S=\boldsymbol{Z}$，则导致K有一个非平凡的赋值，与已知条件相违。所以K的特征$p\neq 0$。又假设K不是$\boldsymbol{Z}/p\boldsymbol{Z}$的代数扩域，则存在对$\boldsymbol{Z}/p\boldsymbol{Z}$超越的元素$x\in K$。于是$K\supset(\boldsymbol{Z}/p\boldsymbol{Z})[x]$。又应用系1，令$S=(\boldsymbol{Z}/p\boldsymbol{Z})[x]$，又得出$K$的一个非平凡赋值。

$\Longleftarrow$。令R_v是K的一赋值环，则$R_v\ni 1$，所以$R_v\supset \boldsymbol{Z}/p\boldsymbol{Z}$。于是$v$是$\boldsymbol{Z}/p\boldsymbol{Z}$赋值。根据定理7.5前面的引理中的1)，立得本系。 ▎

定理7.7(扩充定理) 设L是K的扩域。那么，任给K的赋值环R_v，都存在L的一个赋值环R_w，使

$$R_w\cap K=R_v, \quad \mathfrak{m}_w\cap K=\mathfrak{m}_v,$$

这里$\mathfrak{m}_w$和$\mathfrak{m}_v$分别是R_w和R_v的极大理想。

证明 用上面的定理，存在L的赋值环R_w，使

$$R_w\supset R_v, \quad \mathfrak{m}_w\supset \mathfrak{m}_v.$$

任取$a\in K\backslash R_v$，则$a^{-1}\in \mathfrak{m}_v\subset \mathfrak{m}_w$，所以$a^{-1}$在$R_w$中不是可逆元。因此$a\overline{\in} R_w$，$a\overline{\in} R_w\cap K$。这就证明了$R_w\cap K=R_v$。于是也有

$$\mathfrak{m}_w\cap K=\mathfrak{m}_v. \quad ▎$$

系 设K是k的扩域。那么，K只有平凡的k赋值$\Longleftrightarrow K$是k的代数扩域。

证明 $\Longrightarrow$。任取$a\in K$。如果a对k是超越的，那么，$k(a)$有一个非平凡的k赋值环$k[a]_{(a)}$。根据上面的定理，它可以扩充成K的一个非平凡的k赋值。

$\Longleftarrow$。应用定理7.5前面的引理。 ▎

定理7.7中所说的R_w称为R_v的一个**扩充**，R_v称为R_w在K上

的限制。

例9 设$K=\boldsymbol{C}(x,y)$，$S=\boldsymbol{C}[x,y]_{(x,y)}$。则$S$是一个局部环。我们考虑在$S$上是有限的，而且在$S$的中心是$(x,y)S$的$\boldsymbol{C}$赋值$v$。

根据定理7.5，

$$\text{rank } v+\text{res-dim } v\leqslant 2=\text{tr deg}(K/\boldsymbol{C})。$$

所以$\text{rank } v=1$或2。当$\text{rank } v=1$时，v是一个实赋值(参见例6)，

$$\text{res-dim } v=0 \text{ 或 } 1。$$

v按照其全序群G的性质又可分成三类：1) $G\approx\boldsymbol{Z}$；2) $G\not\approx\boldsymbol{Z}$，$G\approx G^*\subset\boldsymbol{Q}$；3) $G\approx\boldsymbol{Z}+\boldsymbol{Z}r$，此处$r$是一个无理数。我们分别举一些例子如下。

1) $\text{rank } v=1$，$\text{res-dim } v=1$，$G\approx\boldsymbol{Z}$。令

$$R_v=\boldsymbol{C}(x/y)[y]_{(y)}。$$

不难看出，$R_v\supset S$，$\mathfrak{m}_v=yR_v\ni x$，$\mathfrak{m}_v\cap S=(x,y)S$，$R_v$是一维诺德正则局部环，也即是赋值环。又易见$R_v/\mathfrak{m}_v\approx\boldsymbol{C}(x/y)$，故

$$\text{res-dim } v=1。$$

又，如果我们用$x-y^n$代替x，就得出许多不同的例子了。

2) $\text{rank } v=1$，$\text{res-dim } v=0$，$G\approx\boldsymbol{Z}$。定义映射α: $\boldsymbol{C}(x,y)\to\boldsymbol{C}((t))$，$\alpha(x)=t$，$\alpha(y)=te^t$，这里e是对数函数的底。因为$e^t$是超越函数，所以$t$与$te^t$是代数无关的，因此$\alpha$是一个嵌入映射。已知$\boldsymbol{C}[[t]]$是一个一维诺德正则局部环，$\boldsymbol{C}((t))$是它的比域，所以$\boldsymbol{C}[[t]]$是$\boldsymbol{C}((t))$的一个赋值环。不难检验，

$$\boldsymbol{C}[[t]]\supset\alpha(S),\quad t\boldsymbol{C}[[t]]\cap\alpha(S)=\alpha((x,y)S)。$$

令$R_v=\alpha^{-1}(\boldsymbol{C}[[t]]\cap\alpha(\boldsymbol{C}(x,y)))$，即得$R_v$是$\boldsymbol{C}(x,y)$的赋值环。易见

$$\begin{aligned}\boldsymbol{C}\subseteq\boldsymbol{C}[x,y]_{(x,y)}/(x,y)\boldsymbol{C}[x,y]_{(x,y)}&\subset R_v/\mathfrak{m}_v\\&\subset\boldsymbol{C}[[t]]/t\boldsymbol{C}[[t]]=\boldsymbol{C},\end{aligned}$$

所以$R_v/\mathfrak{m}_v=\boldsymbol{C}$，$\text{res-dim } v=0$。又因为$\boldsymbol{C}[[t]]$的全序群是$\boldsymbol{Z}$，不难看出，$v$的全序群也是$\boldsymbol{Z}$。

3) $\mathrm{rank}\, v=1$，$\text{res-dim}\, v=0$，$G\not\approx \boldsymbol{Z}$，$G\approx G^*\subset \boldsymbol{Q}$。类似于 2)的构造方法，令

$$\boldsymbol{C}\langle\langle t\rangle\rangle=\left\{\sum_{n_i\geq m}^{\infty} a_i t^{n_i}：\{n_i\}\text{是}\boldsymbol{Q}\text{的离散子集}\right\}.$$

（所谓离散子集即无极限点的子集。）读者自行证明 $\boldsymbol{C}\langle\langle t\rangle\rangle$ 是一个域。任意取定一个

$$h(t)\in \boldsymbol{C}\langle\langle t\rangle\rangle,\qquad h(t)=\sum_{i=1}^{\infty} a_i t^{n_i},$$

其中 $n_i>0$，诸 n_i 的公分母没有上限。我们定义，对于 $f(x,y)\in \boldsymbol{C}(x,y)$，

$$v(f(x,y))=\mathrm{ord}_t f(t,h(t)).$$

读者自行证明，这就是我们所要的赋值。

4) $\mathrm{rank}\, v=1$，$\text{res-dim}\, v=0$，$G\approx \boldsymbol{Z}+\boldsymbol{Z}r$，$r$ 是无理数。定义映射 β：$\boldsymbol{C}(x,y)\to \boldsymbol{C}(t,t^r)$，$\beta(x)=t$，$\beta(y)=t^r$。定义赋值 v 如下：

$$v(f(x,y))=\mathrm{ord}_t(\beta(f(x,y))).$$

5) $\mathrm{rank}\, v=2$（$\text{res-dim}\, v$ 自然是 0）。取 $G=\boldsymbol{Z}\oplus \boldsymbol{Z}$，用字母全序。定义 $v(x)=(1,0)$，$v(y)=(0,1)$。 ▌

从上面这个例子，我们看到 $\boldsymbol{C}(x,y)$ 有无穷无尽的赋值。这是因为 $\dim S=2>1$ 的关系。我们再举一些比较简单的例子。

例10 1) 讨论在 $\boldsymbol{Z}$ 上有限的赋值。设 $\boldsymbol{Q}$ 的赋值 v 在 $\boldsymbol{Z}$ 上是有限的。令 R_v 是它的赋值环，$\mathfrak{m}_v$ 是 R_v 的极大理想。又令 $(p)=\mathfrak{m}_v\cap \boldsymbol{Z}$。如果 $(p)=(0)$，那么，$\boldsymbol{Z}^*=\boldsymbol{Z}\backslash\{0\}$ 是 R_v 的可逆元集，故 $R_v=\boldsymbol{Q}$，即 v 是平凡赋值。否则，p 是一个素数，$\boldsymbol{Z}\backslash(p)$ 是 R_v 的可逆元集。因此 $R_v\supset \boldsymbol{Z}_{(p)}$，由定理7.4，即有

$$R_v=(\boldsymbol{Z}_{(p)})_{(p)}=\boldsymbol{Z}_{(p)}.$$

于是我们得出了所有在 $\boldsymbol{Z}$ 上有限的赋值。

2) 设 $S=k[x]$，$K=k(x)$，此处 k 是域。设 K 的 k 赋值 v 在

S上是有限的，R_v是它的赋值环，$\mathfrak{m}_v$是R_v的极大理想。令

$$(f(x)) = \mathfrak{m}_v \cap S.$$

与上面一样，我们得出$f(x)=0$或$f(x)$是一个不可约多项式，

$$R_v = K \text{ 或 } R_v = k[x]_{(f(x))}.$$

设K的k赋值在S上不是有限的，那么$x \bar{\in} R_v$（否则，$R_v \supset k$，$x \in R_v \Longrightarrow R_v \supset k[x] = S$），

$$x^{-1} \in \mathfrak{m}_v \subset R_v, \quad R_v \supset k[x^{-1}],$$

$$\mathfrak{m}_v \cap k[x^{-1}] = x^{-1}, \quad R_v = k[x^{-1}]_{(x^{-1})}.$$

从几何学上来看，令$k = \boldsymbol{C}$，那么$f(x) = x - a$，$(a \in \boldsymbol{C})$。于是$\{\boldsymbol{C}(x)$的所有非平凡的$\boldsymbol{C}$赋值$\} \longleftrightarrow \boldsymbol{C} \cup \{\infty\}$ = 黎曼球面。 ▎

赋值的用途之一是下面的定理。

定理7.8 1）赋值环R_v是整数封闭的；

2）任给域K的一个子环S，那么，S在K内的整数闭包$\bar{S}$是在S上有限的所有赋值环的交集；

3）更进一步，设$\mathfrak{p}$是S的一个素理想，$\mathscr{F}$是在S上的中心为$\mathfrak{p}$的所有赋值环的集合，那么

$$S_{\mathfrak{p}}\text{的整数闭包 } \bar{S}_{\mathfrak{p}} = \bigcap_{R_v \in \mathscr{F}} R_v.$$

证明 1）设$x \in K$对R_v是整数相关的，即x适合

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0, \quad a_i \in R_v.$$

如果$x \bar{\in} R_v$，那么$x^{-1} \in R_v$。以x^{n-1}去除上式，得到矛盾的结果：

$$x = -a_1 - a_2 x^{-1} - \cdots - a_n x^{-(n-1)} \in R_v.$$

2）由1），$\bar{S}$含于所有在S上是有限的赋值环里。反过来说，设x不是对S整数相关的，令$y = x^{-1}$，$S' = S[y]$。我们要先说明y不是S'的可逆元。假若它是可逆元，那么，有

$$x = y^{-1} = b_0 y^m + b_1 y^{m-1} + \cdots + b_m, \quad b_i \in S.$$

两边乘以x^m，得

$$x^{m+1} - b_m x^m - \cdots - b_1 x - b_0 = 0,$$

即x对S为整数相关的，这与对x的假设相违。所以y不是S'

的可逆元，故 $yS' \neq S'$。根据定理7.6，存在一个赋值环 R_v，使 $R_v \supset S' \supset S$，$y \in \mathfrak{m}_v$，这里 $\mathfrak{m}_v$ 是 R_v 的极大理想。所以 y 在 R_v 中不是可逆元，即 $x = y^{-1} \overline{\in} R_v$。

3) 应用2)，只要证明"$R_w \supset S_\mathfrak{p} \Longrightarrow$ 存在 $R_v \in \mathscr{F}$，使 $R_w \supset R_v$"就足够了，这里 R_w 是 K 的赋值环。

设 $\mathfrak{m}_w \cap S = \mathfrak{q} \subsetneqq \mathfrak{p}$。在与 w 相伴的位 σ 的作用下，也就是在典型映射 σ: $R_w \to R_w/\mathfrak{m}_w = K_1$ 的作用下，记

$$S_1 = \sigma(S_\mathfrak{p}), \quad \mathfrak{p}_1 = \sigma(\mathfrak{p}S_\mathfrak{p}),$$

则 $\mathfrak{p}_1$ 是 S_1 的极大理想。于是，存在 K_1 的一个赋值 u，使

$$R_u \supset S_1, \quad \mathfrak{m}_u \cap S_1 = \mathfrak{p}_1.$$

令 $R_v = \sigma^{-1}(R_u)$，显然有 $R_w \supset R_v \supset S$。我们要说明 R_v 是一个赋值环及 $\mathfrak{m}_v \cap S = \mathfrak{p}$。任取 $a \overline{\in} R_v$。如果 $a \in R_w$，则

$$a \overline{\in} R_v \Longleftrightarrow \sigma(a) \overline{\in} R_u \Longrightarrow \sigma(a)^{-1} \in R_u \Longrightarrow a^{-1} \in R_v.$$

如果 $a \overline{\in} R_w$，则 $a^{-1} \in \mathfrak{m}_w$，于是

$$\sigma(a^{-1}) = 0 \in R_u \Longrightarrow a^{-1} \in R_v.$$

所以 R_v 是赋值环。我们又有

$$\mathfrak{m}_v \cap S = \mathfrak{p} \Longleftrightarrow \mathfrak{m}_v \cap S_\mathfrak{p} = \mathfrak{p}S_\mathfrak{p} \Longleftrightarrow \mathfrak{m}_u \cap S_1 = \mathfrak{p}_1. \quad \blacksquare$$

系 如果 S 是整数封闭的，那么 $S_\mathfrak{p} = \bigcap_{R_v \in \mathscr{F}} R_v$。 $\blacksquare$

习　题

1. 在 $\mathbf{Q}$ 内找一个赋值 v，使满足下列两条件中某一条：

(1) $R_v \supset \mathbf{Z}$，$\mathfrak{m}_v \cap \mathbf{Z} \supset 6\mathbf{Z}$，

(2) 令 $S = \mathbf{Z}_{(7)}$。$R_v \supset S$，$\mathfrak{m}_v \cap S = 7S$。

2. 在 $\mathbf{Q}(\mathrm{i})$ 内找一个赋值 v，使

$$R_v \supset \mathbf{Z}[\mathrm{i}], \quad \mathfrak{m}_v \cap \mathbf{Z}[\mathrm{i}] = (2+\mathrm{i})\mathbf{Z}[\mathrm{i}].$$

3. 在 $\mathbf{Q}$ 内给定赋值环 $S = \mathbf{Z}_{(7)}$。试在 $\mathbf{Q}(\mathrm{i})$ 内找出赋值 w，使

$$R_w \cap \mathbf{Q} = S \text{ 和 } \mathfrak{m}_w \cap \mathbf{Q} = 7S.$$

4. 设k为域，在$k(x,y)$内考虑子环$k[x,y]$对素理想(x)的局部化环$S=k[x,y]_{(x)}$。试求$k(x,y)$的一个赋值v，使得$R_v\supset S$，且$\mathfrak{m}_v\cap S=(x)S$。

5. 设R是域K的子环但不是域，而且不存在K的非域子环真包含R(即R具有极大性)，证明R是K的一个赋值环。

6. 设R是域K的子环，$\mathfrak{p}$是R的一个真素理想。证明存在K的一个赋值环R_v，使$R_v\supset R$且$\mathfrak{m}_v\cap R=\mathfrak{p}$。

7. 利用上一题证明：设R是整环，S是R的子环，R对S整数相关，那么对S内任一素理想$\mathfrak{p}$，存在R内素理想$\mathfrak{q}$，使

$$\mathfrak{q}\cap S=\mathfrak{p}.$$

8. 试求一整环S，它整数封闭，但不是它的比域的赋值环。

9. 设p为素数，$\boldsymbol{Z}_{(p)}$为$\boldsymbol{Z}$对(p)的局部化环，证明

$$\bigcap_{\text{对一切 } p}\boldsymbol{Z}_{(p)}=\boldsymbol{Z}.$$

10. 参考例9的3)，证明$\boldsymbol{C}\langle\langle t\rangle\rangle$是一个域。

11. 令

$$K[\langle t\rangle]=\left\{\sum a_i t^i:\ a_i\in\boldsymbol{Q},\ \text{所有 } a_i\neq 0 \text{构成}\boldsymbol{Q}\text{的良序子集}\right\}.$$

证明$K[\langle t\rangle]$是一个域。

12. 设R是环S的子环，$x_1,\cdots,x_n\in S$，满足下列方程：

$$x_i^{n_i}+f_i(x_1,\cdots,x_n)=0,$$

其中$f_i(y_1,\cdots,y_n)\in R[y_1,\cdots,y_n]$，$\deg f_i(y_1,\cdots,y_n)<n_i$。证明$x_1,\cdots,x_n$对$R$都是整数相关的。

13. 任取$m/n\in\boldsymbol{Q}$，$(m,n)=1$，$n\neq\pm1$。用定理7.8证明m/n不是对$\boldsymbol{Z}$整数相关的。

14. 判断x/y^3是否对$\boldsymbol{C}\left[\dfrac{x^2-y^3}{x},\dfrac{x}{y}\right]$整数相关。

§3 实赋值

设v是域K的一个非平凡的实赋值，这就是说，它的全序群$G_v \subset \mathbf{R}$，$G_v \neq \{0\}$。也等于说，rank $v=1$。读者请参见例6及例7。此时域K称为一个赋值域。我们用v定义一个绝对值“$|\ |_v$”：

$$\left.\begin{array}{l}|a|_v = e^{-v(a)},\\ |0|_v = e^{-\infty} = 0.\end{array}\right. \quad e>1;$$

此处，e不一定是自然对数的底。那么，它适合：

1*) $|ab|_v = |a|_v |b|_v$；

2*) $|a+b|_v \leqslant \max\{|a|_v, |b|_v\}$，

而赋值环$R_v = \{a: |a|_v \leqslant 1\}$，$R_v$的极大理想$\mathfrak{m}_v = \{a: |a|_v < 1\}$。应用1*)及2*)，我们在$K$里定义一个距离$d_v$如下：

$$d_v(a,b) = |a-b|_v.$$

不难看出，d_v适合距离的三个条件：

1) $d_v(a,b) \geqslant 0$，且$d_v(a,b)=0 \Longleftrightarrow a=b$；

2) $d_v(a,b) = d_v(b,a)$；

3) $d_v(a,c) \leqslant d_v(a,b) + d_v(b,c)$。

（事实上，可以用强三角不等式代替3）。）因此，对d_v而言，K是一个度量空间。于是，我们可以通过柯西序列$\{a_i\}$得到K的完备化集$\hat{K}$。请注意，嵌入映射α：$K \to \hat{K}$，即是$\alpha(a) = \{a, a, \cdots, a, \cdots\} = \{a\}$。如通常一样，$\hat{\hat{K}} = \hat{K}$，即$\hat{K}$是一个完备化集。请参见第一章§6及第六章§8。

定理7.9 1) $\hat{K}$是一个域。任给K的柯西序列$\{a_i\}$，定义

$$v(\{a_i\}) = \lim_{i\to\infty} v(a_i),$$

则$v(\{a_i\})$是$\hat{K}$的一个赋值，仍然用v表示之。

2) $R_v/\mathrm{m}_v \approx \hat{R}_v/\hat{\mathrm{m}}_v$，$G_v=\hat{G}_v=\{v(\{a_i\}):\ \{a_i\}\in\hat{K}\}$。

证明 1) 不难看出$\hat{K}$是一个环．我们仅证$\hat{K}$的每一个非零元素$\{a_i\}$都是可逆元．任给$0<\varepsilon\in\boldsymbol{R}$，都存在一个正整数$N(\varepsilon)$，使

$$n,l>N(\varepsilon)\implies |a_n-a_l|_v<\varepsilon.$$

于是显见存在正整数L，使

$$l>L\implies |a_l|_v\geqslant r>0.$$

令$b_i=1(\forall 1\leqslant i\leqslant L)$，$b_i=a_i^{-1}(\forall i>L)$．则

$$\{a_i\}\{b_i\}=\{a_1,\cdots,a_L,1,\cdots,1,\cdots\}\sim\{1\}.$$

现在我们只要证明$\{b_i\}$是柯西序列便足够了．当$n,l>\max\{N(\varepsilon),L\}$时，有

$$|b_n-b_l|_v=\left|\frac{a_l-a_n}{a_na_l}\right|_v\leqslant r^{-2}\varepsilon.$$

故$\{b_i\}$是柯西序列。

显然，$v(\{a_i\})=\lim\limits_{i\to\infty}v(a_i)$是$\hat{K}$的一个赋值．

2) 我们先证$G_v=\hat{G}_v$．因为

$$v(\{a\})=\lim v(a)=v(a),$$

所以$G_v\subset\hat{G}_v$．反之，假设有$l\in\hat{G}_v\backslash G_v$，那么$l=v(\{a_i\})$必然是$G_v$的一个极限点．我们可以选取$\{a_i\}$的一个子序列$\{b_i\}$，使$v(b_i)$皆不相同．于是当$i,j$充分大时(无妨设$v(b_i)<v(b_j)<l+1$)，有（参见定理7.2)

$$v(b_i-b_j)=\min\{v(b_i),v(b_j)\}=v(b_i)<l+1,$$

即$d_v(b_i,b_j)>e^{-l-1}>0$．所以$\{b_i\}$没有极限(实际上证明了一个较强的事实：如果$\lim|a_i|_v\neq 0$，此处$\{a_i\}$是一个柯西序列，那么，$v(a_i)$当i充分大后必取一定值)。

我们现在证明$R_v/\mathrm{m}_v\approx\hat{R}_v/\hat{\mathrm{m}}_v$．不难看出，由嵌入映射

$$\sigma:\ K\to\hat{K}$$

诱导出R_v/m_v到$\hat{R}_v/\hat{\mathrm{m}}_v$的一个环映射．由于二者是域，所以仅须说明这个环映射是满射．设有柯西序列$\{a_i\}\in\hat{R}_v\backslash\hat{\mathrm{m}}_v$，则$v(\{a_i\})$

$=0$。由于$\{a_i\}$是柯西序列，所以必存在正整数l，使

$$v(a_i-a_j)>0, \quad \forall i,j\geqslant l.$$

由我们在证明1)的最后所作的说明，不妨假定

$$v(a_i)=0, \quad \forall i\geqslant l.$$

于是$a_l\in R_v$，而且$v(a_i-a_l)>0(\forall i\geqslant l)\Longrightarrow v(\{a_i\}-\{a_l\})>0$
$\Longrightarrow\{a_i\}-\{a_l\}\in\hat{\mathfrak{m}}_v$，即$\{a_l\}$在$\hat{R}_v/\hat{\mathfrak{m}}$中的象与$\{a_i\}$的象相同，也即前面所说环映射是满射。▌

例11 设$\hat{K}$是如上所述的完备域。考虑

$$\hat{K}\{\{x_1,\cdots,x_n\}\}=\left\{\sum f_{i_1\cdots i_n}x_1^{i_1}\cdots x_n^{i_n}:\ 存在A,L\in\boldsymbol{R},\ 使\ |f_{i_1\cdots i_n}|_v\leqslant AL^{i_1+\cdots+i_n}\right\}$$
$$\subset\hat{K}[[x_1,\cdots,x_n]].$$

我们可以定义$f(x_1,\cdots,x_n)\in\hat{K}\{\{x_1,\cdots,x_n\}\}$的收敛半径如下：设

$$f(x_1,\cdots,x_n)=\sum f_{i_1\cdots i_n}x_1^{i_1}\cdots x_n^{i_n},$$

那么，它的收敛半径是

$$r=\sup\{L^{-1}:\ 存在A\in\boldsymbol{R},\ 使|f_{i_1\cdots i_n}|_v\leqslant AL^{i_1+\cdots+i_n}\}.$$

显然，$r>0$。我们要说明，只要$|a_i|_v<r(\forall i=1,\cdots,n)$，那么$f(a_1,\cdots,a_n)\in\hat{K}$。这就是说，在原点$(0,\cdots,0)$附近可以计算$f(a_1,\cdots,a_n)$。设$a=\max\{|a_i|_v\}$，则$a<r$。故存在$A,L$，使$a<L^{-1}<r$且$|f_{i_1\cdots i_n}|_v\leqslant AL^{i_1+\cdots+i_n}$。令$f(x_1,\cdots,x_n)$的部分和为

$$f_l^*(x_1,\cdots,x_n)=\sum_{i_1+\cdots+i_n<l}f_{i_1\cdots i_n}x_1^{i_1}\cdots x_n^{i_n}.$$

那么，按照强三角不等式，有

$$|f(a_1,\cdots,a_n)-f_l^*(a_1,\cdots,a_n)|_v\leqslant A(aL)^l.$$

所以
$$f(a_1,\cdots,a_n)=\lim_{l\to\infty}f_l^*(a_1,\cdots,a_n)\in\hat{K}.$$

这与初等分析学的方法是一致无二的。

我们考虑三个代数实体：

$$\hat{K}[x_1,\cdots,x_n]\subset\hat{K}\{\{x_1,\cdots,x_n\}\}\subset\hat{K}[[x_1,\cdots,x_n]].$$

在谱集的意义下，三者都建立了几何学，即代数几何学、解析几何学及形式几何学。在解方程式的意义下，$\hat{K}[x_1,\cdots,x_n]$中元素的解是全局性的，$\hat{K}\{\{x_1,\cdots,x_n\}\}$的元素求解是在微区内进行的，而形式幂级数的解是沒有意思的。▎

设域K上有n个实赋值$v_1,\cdots,v_n$，各自在K上定义了一个距离$d_{v_1},\cdots,d_{v_n}$，各自引生了一个拓扑。这些拓扑之间有沒有什么关系？我们看一些例子。令$K=\mathbf{Q}$。在第一章§4，我们研究了中国剩余定理。设d_i是与素数p_i相对应的距离。由中国剩余定理，对于任给的$a_i\in\boldsymbol{Z}$，下面的一组同余式有解：

$$x\equiv a_i(\bmod p_i^{m_i}),\quad i=1,\cdots,n.$$

换句话说，即存在$x\in\boldsymbol{Z}$，使

$$d_i(x,a_i)<e^{-m_i},\quad \forall i=1,\cdots,n,$$

这里e是一个大于1的实数。这也就是说，x对这些不同的拓扑而言，可以同时逼近$a_1,\cdots,a_n$到任何精确度。这表现了这些拓扑的独立性。我们再看另外一个例子。

例12 复变函数中有所谓"Mittag-Leffler 定理"：任给$\mathbf{C}$的一个离散子集$\{a_i\}$及在每一个a_i附近的一个亚纯函数的主部

$$g_i(x-a_i)=\sum_{j=1}^{s_i}a_{ij}(x-a_i)^{-j},$$

那么，存在一个亚纯函数$f(x)$，使得：1）它在$\{a_i\}$之外是全纯的；2）g_i是它在a_i的主部。

令$K=\{$极点集是离散的亚纯函数$\}\cup\{0\}$。用黎曼定理，我们可以证明K是域。令

$$v_a(f(x))=\mathrm{ord}_{x-a}(f(x)),\quad f(x)\in K.$$

不难看出，v_a是K的一个赋值。我们可以把 Mittag-Leffler 定理的结论改写如下：

$$d_{v_b}(f)\leqslant 1,\qquad \forall b\bar{\in}\{a_i\};$$

$$d_{v_a}(f-g_i)\leqslant 1,\qquad \forall a\in\{a_i\}.\ \blacksquare$$

与例12不同的，在代数学中，只处理有限多个赋值 $v_1,\cdots,v_n$。我们先证明下面的引理。

引理 设 $v_1,\cdots,v_n$ 是 K 的不等价的赋值，即 $R_{v_i}\neq R_{v_j}$ $(i\neq j)$。

1) 如果 v_i 都是一秩的，那么 $R_{v_i}\not\subset R_{v_j}$ $(\forall i\neq j)$；

2) 如果 $R_{v_i}\not\subset R_{v_j}$ $(\forall i\neq j)$，那么，存在 $b_1,\cdots,b_n\in K$，使得

$$b_i\in R_{v_i}\setminus m_{v_i}\ (\forall i=1,2,\cdots,n),\qquad b_i\in \mathfrak{m}_{v_j}\ (\forall j\neq i).$$

此处 $\mathfrak{m}_{v_i}$ 是 R_{v_i} 的极大理想。

证明 1) 假设 $R_{v_i}\subset R_{v_j}$，那么，根据定理7.4，

$$R_{v_j}=(R_{v_i})_{\mathfrak{p}},$$

其中 $\mathfrak{p}=\mathfrak{m}_{v_j}\cap R_{v_i}$。由于 R_{v_i} 是一秩的，所以 $\mathfrak{p}=(0)$或 $\mathfrak{m}_{v_i}$，故 $R_{v_j}=K$ 或 R_{v_i}。

2) 先考虑 $n=2$ 的情形。已知 $R_{v_1}\not\subset R_{v_2}$，那么，存在 $c\in R_{v_1}\setminus R_{v_2}$。如果 $c\in R_{v_1}\setminus\mathfrak{m}_{v_1}$，那么

$$b_1=c^{-1}\in R_{v_1}\setminus\mathfrak{m}_{v_1},\quad b_1\in \mathfrak{m}_{v_2}.$$

b_1即符合引理的要求。如果 $c\in\mathfrak{m}_{v_1}$，则$1+c\in R_{v_1}\setminus R_{v_2}$且$1+c\in R_{v_1}\setminus m_{v_1}$，那么$b_1=(1+c)^{-1}\in R_{v_1}\mathfrak{m}_{v_1}$，$b_1\in\mathfrak{m}_{v_2}$。同法可作出$b$

考虑 $n>2$ 的情形。用归纳法。假设已经解决 $n-1$ 的情形，即存在 $c\in R_{v_1}\setminus\mathfrak{m}_{v_1}$，$c\in\mathfrak{m}_{v_j}$ $(j=2,\cdots,n-1)$。我们先找一个 c_n，使$c_n\in R_{v_1}\setminus\mathfrak{m}_{v_1}$，$c_n\in\mathfrak{m}_{v_j}$ $(j=2,\cdots,n-1)$，且$c_n\in R_{v_n}$。如果 $c\in R_{v_n}$，即令 $c_n=c$。如果 $c\bar{\in}R_{v_n}$，我们考虑几种可能性：令 σ：$R_{v_1}\to R_{v_1}/\mathfrak{m}_{v_1}$ 为典型映射，

(a) 如果 $\sigma(c)\neq 1$，我们令 $c_n=c/(c-1)$；

(b) 如果 $\sigma(c)=1$， $\sigma(R_{v_1})$的特征$\neq 2$，我们令

$$c_n = c/(c+1);$$

(c) 如果 $\sigma(c)=1$， $\sigma(R_{v_1})$的特征$=2$，我们令

$$c_n = (c^3+c^2+c)/(c^3+c+1).$$

通过对 c_n 的各个赋值的简单计算，即知 c_n 符合上面的要求。同样地，我们找出 $c_i(i=2,\cdots,n-1)$，使

$$c_i \in R_{v_1} \setminus \mathrm{m}_{v_1}, \quad c_i \in \mathrm{m}_{v_j} (j \neq 1, i), \quad c_i \in R_{v_i}.$$

令

$$b_1 = \prod_{i=2}^{n} c_i,$$

则 b_1即符合本引理的要求。同法可求出 $b_2,\cdots,b_n$。 ▌

讨论 令 $K=\mathbf{Q}$，$R_{v_i}=\boldsymbol{Z}_{(p_i)}$。请把上面的引理与中国古代的“大衍求一”相比。

定理7.10(逼近定理) 设 $v_1,\cdots,v_n$是域K的实赋值，$G_1,\cdots,G_n\subset \boldsymbol{R}$ 是它们的全序群。我们任给 $a_1,\cdots,a_n\in K$，$l_1\in G_1$，$\cdots$，$l_n\in G_n$。那么，存在$a\in K$，使

$$v_i(a-a_i)=l_i, \quad \forall i=1,\cdots,n.$$

证明 我们分成几段来证明。

1) 只要证明对任意的整数 l，都存在相应的 $c\in K$，使得

$$v_i(c-a_i)\geqslant l, \quad \forall i=1,2,\cdots,n \tag{1}$$

便足够了。这因为，我们可以取 $l>l_i(\forall i)$。任取 d_i，使 $v_i(d_i)=l_i$。那么，存在 d，使

$$v_i(d-d_i)\geqslant l>l_i, \quad \forall i=1,2,\cdots,n.$$

而 $d=(d-d_i)+d_i$，所以

$$v_i(d)=l_i, \quad \forall i=1,2,\cdots,n.$$

又设 c 适合(1)式，令 $a=c+d$，则有

$$v_i(c+d-a_i)=v_i(d)=l_i, \quad \forall i=1,2,\cdots,n.$$

2) 应用上面的引理，存在 $b_1,\cdots,b_n\in K$，使

$$v_i(b_i)=0, \; v_j(b_i)>0, \quad \forall j\neq i.$$

令 $e_i = b_i \Big/ \sum_{j=1}^{n} b_j$. 则

$$v_i(e_i) = 0,\ v_j(e_i) > 0, \qquad \forall j \neq i.$$

而且在典型映射 σ_i: $R_{v_i} \to R_{v_i}/\mathfrak{m}_{v_i}$ 作用下，$\sigma_i(e_i) = 1$。于是

$$v_i(e_i - 1) > 0 \quad (\forall i).$$

3) 令正整数 s 适合下列不等式:

$$sv_i(e_i - 1) + v_i(a_i) \geq l, \qquad \forall i = 1, \cdots, n, \tag{2}$$

$$sv_j(e_i) + v_j(a_i) \geq l, \qquad \forall j \neq i. \tag{3}$$

取 $f_i \in K$ 如下:

$$f_i = 1 - (1 - e_i^s)^s, \qquad i = 1, \cdots, n.$$

那么

$$\begin{aligned}(4)\quad v_i(a_i(f_i - 1)) &= v_i(f_i - 1) + v_i(a_i) = sv_i(1 - e_i^s) + v_i(a_i)\\ &= s(v_i(1 - e_i) + v_i(1 + e_i + \cdots + e_i^{s-1})) + v_i(a_i)\\ &\geq sv_i(1 - e_i) + v_i(a_i) \geq l.\end{aligned}$$

同时，我们可以看出 $f_i = e_i^s g(e_i^s)$，此处 $g(x)$ 为整系数多项式。所以 $v_j(f_i) \geq sv_j(e_i)$。代入(3)式，立得

$$v_j(f_i a_i) \geq l. \tag{5}$$

令 $c = f_1 a_1 + f_2 a_2 + \cdots + f_n a_n$。应用 (4)及(5)式，立得(1)式。 ∎

讨论 1) 上面的定理可以看成中国剩余定理的一般化。

2) 上面的定理说明了实赋值的独立性。对任意的赋值 $v_1, \cdots, v_n$ 而言，当 $R_{v_i} \not\subset R_{v_j}$ ($\forall i \neq j$)时，我们称它们是**独立的**。那么，只要它们是独立的，上面的定理还是成立的。

3) 应用上面的定理到 $\mathbf{C}(x)$上，我们得出一个类似于Mittag-Leffler 定理的命题。读者试讨论之。

习 题

1. 设v_2, v_3, v_5, v_7是$\mathbf{Q}$内由素数2,3,5,7决定的赋值。试在$\mathbf{Q}$内找一a，使$v_i(a - i) = i$。

2. 在有理函数域$\mathbf{Q}(x)$内由不可约多项式

$$f(x)=x^2+x+1; \quad g(x)=x^3-2$$

定义两个赋值v_1, v_2：

$$v_1\left(f(x)^l\frac{m(x)}{n(x)}\right)=l, \quad (m(x),f(x))=(n(x),f(x))=1;$$

$$v_2\left(g(x)^l\frac{m(x)}{n(x)}\right)=l, \quad (m(x),g(x))=(n(x),g(x))=1.$$

试求$h(x)\in \boldsymbol{Q}(x)$，使

$$v_1(h(x))=-2, \quad v_2(h(x))=2.$$

3. 给定域K的互不等价的实赋值$v_1,\cdots,v_n$，证明对任意不全为零的整数$l_1,\cdots,l_n$，关系式

$$l_1v_1(x)+\cdots+l_nv_n(x)=0$$

不可能对一切K内的非零元素x都成立。

4. 试求$\boldsymbol{R}(x)$对赋值$\boldsymbol{R}[x]_{(x^2+1)}$的完备化域。

5. 在$\boldsymbol{C}(x)$内，由赋值环$\boldsymbol{C}[x]_{(x-n)}$ $(n=1,2,3)$决定的赋值记为v_n。试求$f(x)\in \boldsymbol{C}(x)$，使

$$v_n\left(f(x)-\frac{1}{(x-n)^n}\right)=n \quad (n=1,2,3).$$

6. 设K是一个完备域，令

$$(*) \qquad a_0+a_1x+\cdots \qquad (a_i\in K)$$

是K上的一个幂级数。以$|a|$ $(a\in K)$表K内的乘法实赋值。若对$x\in K$，幂级数

$$|a_0|+|a_1||x|+\cdots$$

在$\boldsymbol{R}$内收敛，则称(*)在点x处绝对收敛。证明：存在实数$r\geqslant 0$，使当$|x|<r$时(*)绝对收敛，而当$|x|>r$时不收敛。r称为(*)的收敛半径。

7. 续上题。令

$$l=\overline{\lim_{n\to+\infty}}|a_n|^{1/n}.$$

证明$r=1/l$。

8. 令$R=\mathbf{C}[x,y]/(y^2+2x-1)$，又取$R$的两个极大理想

$$\mathfrak{m}_1=(\bar{x}-1,\bar{y}-i),\quad \mathfrak{m}_2=(\bar{x}-1,\bar{y}+i)$$

($\bar{x},\bar{y}$为x,y在R内的象)．由$R_{\mathfrak{m}_1},R_{\mathfrak{m}_2}$所决定的$R$的比域$K$的赋值分别记为$v_1,v_2$。试在$K$内找一元素$a$，使

$$v_1(a-1)>0,\quad v_2(a+1)\leqslant 0.$$

9. 设域K代数封闭，具有实赋值v，证明K对v的完备化域也是代数封闭的。

§4 Hensel 引理

在有理数域$\mathbf{Q}$里，我们有普通的绝对值"$|\ |$"及实赋值v_p(它的赋值环是$\mathbf{Z}_{(p)}$)。我们可对它们取完备化域，得出$\mathbf{R}$及$\mathbf{Q}_p$(p-adic 数域)。从纯理论的观点来看，$\mathbf{R}$及$\mathbf{Q}_p$都是一样可用的。于是发生了求解$\mathbf{Q}_p[x]$的方程式的问题。显然，下面的方程式

$$x^n-p=0\quad(n>1)$$

在$\mathbf{Q}_p$中无解。这因为，设$a^n-p=0$，$a\in\mathbf{Q}_p$，则

$$nv_p(a)=v_p(a^n)=v_p(p)=1.$$

故$v_p(a)=1/n$，但$1/n\notin\mathbf{Z}=G_{v_p}$，矛盾。所以，完备域$\mathbf{Q}_p$不是代数封闭的。但是，$x^2+2\in\mathbf{Q}_3[x]$在$\mathbf{Q}_3$里有沒有根呢？答案是肯定的。下面的 Hensel 引理，可以部分地回答这类问题。我们先证明一个引理。

引理 设$\delta(x)$是$R[x]$中的首一多项式，此处R是一个环。J是R的一个理想。任取$q(x)\in J[x]$，那么，存在$d(x),r(x)\in J[x]$，使

$$q(x)=d(x)\delta(x)+r(x),\quad \deg r(x)<\deg\delta(x).$$

证明 用欧几里得算法，立得。 ▎

定理7.11(Hensel 引理) 设域K对离散实赋值v是完备的。又设σ: $R_v\to R_v/\mathfrak{m}_v$是典型映射，$\sigma(a)=\bar{a}$。对$f(x)\in R_v[x]$，

令$\sigma(f(x))=\bar{f}(x)$。如果$f(x)$是首一多项式，且

$$\bar{f}(x)=\bar{\gamma}(x)\bar{\delta}(x)\in(R_v/\mathfrak{m}_v)[x],$$

其中$\bar{\gamma}(x),\bar{\delta}(x)$均是$(R_v/\mathfrak{m}_v)[x]$中的首一多项式，且

$$(\bar{\gamma}(x),\bar{\delta}(x))=(1)。$$

那么，存在$R_v[x]$中的两个首一多项式$g(x),h(x)$，使得$\bar{g}(x)=\bar{\gamma}(x)$，$\bar{h}(x)=\bar{\delta}(x)$，且

$$f(x)=g(x)h(x)。$$

证明 由于$(\bar{\gamma}(x),\bar{\delta}(x))=(1)$，所以一定存在$\bar{\alpha}(x),\bar{\beta}(x)\in(R_v/\mathfrak{m}_v)[x]$，使得

$$\bar{\alpha}(x)\bar{\gamma}(x)+\bar{\beta}(x)\bar{\delta}(x)=1。$$

应用欧几里得算法，令

$$\bar{\alpha}(x)=\bar{d}(x)\bar{\delta}(x)+\overline{\alpha'}(x),\quad \deg\overline{\alpha'}(x)<\deg\bar{\delta}(x),$$

再令$\overline{\beta'}(x)=\bar{\beta}(x)+\bar{d}(x)\bar{\gamma}(x)$，则有

$$\overline{\alpha'}(x)\bar{\gamma}(x)+\overline{\beta'}(x)\bar{\delta}(x)=1。$$

不难看出，$\deg\overline{\beta'}(x)<\deg\bar{\gamma}(x)$。我们可令$\bar{\alpha}(x)=\overline{\alpha'}(x)$，$\bar{\beta}(x)=\overline{\beta'}(x)$。取$\gamma(x)$，$\delta(x)$为$R_v[x]$的首一多项式，使

$$\deg\gamma(x)=\deg\bar{\gamma}(x),\quad \deg\delta(x)=\deg\bar{\delta}(x),$$

$$\sigma(\gamma(x))=\bar{\gamma}(x),\quad \sigma(\delta(x))=\bar{\delta}(x)。$$

类似地选取$\bar{\alpha}(x)$及$\bar{\beta}(x)$在$R_v[x]$中的原象$\alpha(x)$及$\beta(x)$，使它们的次数对应相等。于是有

$$\alpha(x)\gamma(x)+\beta(x)\delta(x)\equiv 1 \bmod \mathfrak{m}_v[x]。\tag{1}$$

令$g_0(x)=\gamma(x)$，$h_0(x)=\delta(x)$。我们要逐步构造出$g_n(x)$及$h_n(x)(n=0,1,\cdots)$，使

1) $g_n(x),h_n(x)$(皆$\in R_v[x]$)都是首一多项式，且
$$\deg g_n(x)+\deg h_n(x)=\deg f(x);$$

2) $f(x)\equiv g_n(x)h_n(x)(\bmod \mathfrak{m}_v^{n+1}[x])$;

3) $\bar{g}_n(x)=\bar{\gamma}(x)$，$\bar{h}_n(x)=\bar{\delta}(x)$;

4) $g_n(x)-g_{n-1}(x)\in\mathfrak{m}_v^n(x)(n\geqslant 1)$。

在这些条件下，令$g(x)=\lim g_n(x)$，$h(x)=\lim h_n(x)$，则$g(x)$，

$h(x)$就符合定理的要求。

用归纳法。上面已有 $g_0(x), h_0(x)$。现在假设我们已经作出了 $g_n(x), h_n(x)$。则

(2) $$s_n(x) = f(x) - g_n(x)h_n(x) \in \mathfrak{m}_v^{n+1}[x].$$

以 $s_n(x)$乘(1)式，有

(3) $$s_n(x) \equiv \alpha(x)\gamma(x)s_n(x) + \beta(x)\delta(x)s_n(x) \pmod{\mathfrak{m}_v^{n+2}[x]}.$$

应用引理，存在 $d(x)$及 $a_n(x) \in \mathfrak{m}_v^{n+1}[x]$，使

(4) $$\alpha(x)s_n(x) = d(x)\delta(x) + a_n(x), \quad \deg a_n(x) < \deg \delta(x).$$

令

(5) $$\beta_n^*(x) = \beta(x)s_n(x) + d(x)\gamma(x).$$

我们来考察 $\beta_n^*(x) (\bmod\ \mathfrak{m}_v^{n+2}[x])$的次数。令

$$\tau: R_v[x] \to (R_v/\mathfrak{m}_v^{n+2})[x]$$

为由典型映射 $R_v \to R_v/\mathfrak{m}_v$ 诱导出的环映射，对 $l(x) \in R_v[x]$，记 $\tau(l(x)) = \bar{l}(x)$。由(5)式，有

(6) $$\beta(x)s_n(x) = -d(x)\gamma(x) + \beta_n^*(x).$$

将$\gamma(x) \times (4) + \delta(x) \times (6)$，即有

$$\alpha(x)\gamma(x)s_n(x) + \beta(x)\delta(x)s_n(x) = \gamma(x)a_n(x) + \delta(x)\beta_n^*(x).$$

根据(3)式，即有

(7) $$\bar{s}_n(x) = \bar{\gamma}(x)\bar{a}_n(x) + \bar{\delta}(x)\bar{\beta}_n^*(x).$$

根据上面的条件 1)及(1)式，知 $\deg s_n(x) < \deg f(x)$，故

(8) $$\deg \bar{s}_n(x) < \deg f(x).$$

再由(4)式的 $\deg a_n(x) < \deg \delta(x)$，以及 $\deg \gamma(x) + \deg \delta(x) = \deg f(x)$，知

(9) $$\deg(\bar{\gamma}(x)\bar{a}_n(x)) < \deg f(x).$$

由(7),(8),(9)三式即有

$$\deg \bar{\delta}(x) + \deg \bar{\beta}_n^*(x) < \deg f(x).$$

但 $\delta(x)$是首一多项式，所以 $\deg \bar{\delta}(x) = \deg \delta(x)$，于是

$$\deg \bar{\beta}_n^*(x) < \deg f(x) - \deg \delta(x) = \deg \gamma(x).$$

又，由(5)式，$\beta_n^*(x) \in \mathfrak{m}_v^{n+1}[x]$，所以可以适当选取$\bar{\beta}_n^*(x)$在 τ 作用

下的反象 $\beta_n(x)\in \mathfrak{m}_v^{n+1}[x]$ (即 $\beta_n(x)\equiv\beta_n^*(x) \pmod{\mathfrak{m}_v^{n+2}[x]}$),使

$$\deg \beta_n(x)<\deg \gamma(x).$$

令

$$g_{n+1}(x)=g_n(x)+\beta_n(x),\qquad h_{n+1}(x)=h_n(x)+a_n(x).$$

我们只验证 $g_{n+1}(x)$ 与 $h_{n+1}(x)$ 适合条件 2),其余各条都是自明的:

$$\begin{aligned}
f(x)-g_{n+1}(x)h_{n+1}(x)&=f(x)-(g_n(x)+\beta_n(x))(h_n(x)+a_n(x))\\
&\equiv s_n(x)-\beta_n^*(x)h_n(x)-a_n(x)g_n(x)\\
&\equiv s_n(x)(1-(a(x)\gamma(x)+\beta(x)\delta(x)))\\
&\quad -d(x(\delta(x)\gamma(x)-\gamma(x)\delta(x))\\
&\equiv 0 \pmod{\mathfrak{m}_v^{n+2}[x]}.
\end{aligned}$$ ▎

讨论 上文提到 $x^2+2\in \mathbf{Q}_3[x]$ 在 $\mathbf{Q}_3$ 中有根。事实上,

$$x^2+\bar{2}=(x+\bar{1})(x+\bar{2})\in(\mathbf{Z}/3\mathbf{Z})[x],$$

符合上面定理的条件,因此 x^2+2 在 $\mathbf{Q}_3[x]$ 中可以分解成一次式的乘积。▎

下面是一个在复变函数论及代数几何学中有意义的定理。

定理7.12(Newton-Puiseux 定理) 设 K 是一个特征零的代数封闭域。那么,并集

$$\bigcup_{n=1}^{\infty} K((x^{1/n}))$$

是 $K((x))$ 的代数闭包。

证明 1) $K((x^{1/n}))=K((x))[x^{1/n}]$,所以,$K((x^{1/n}))$ 的每一个元素都是对 $K((x))$ 的代数元。又显然有

$$K((x^{1/n}))\cup K((x^{1/l}))\subset K((x^{1/nl})).$$

由此即知,$\bigcup_{n=1}^{\infty} K((x^{1/n}))$ 是一域,因此它是 $K((x))$ 的一代数扩域。

2) 任取一个关于变数 y 的多项式 $f(y)\in K[[x]][y]$。我们只要证明 $f(y)$ 在

$$\bigcup_{n=1}^{\infty} K((x^{1/n}))$$

中有解就足够了。(为什么？)

设$f(y)=0$的展开式如下($n>1$)：

(1) $a_0(x)y^n+a_1(x)y^{n-1}+\cdots+a_n(x)=0$, $a_i(x)\in K[[x]]$.

用$a_0(x)^{n-1}$乘上式，并用$a_0(x)y$取代y，即不妨设$f(y)$是首一多项式，即有

(2) $y^n+b_1(x)y^{n-1}+\cdots+b_n(x)=0$, $\quad b_i(x)\in K[[x]]$.

我们用y取代$y+\frac{1}{n}b_1(x)$，即不妨设$b_1(x)=0$。令

$$v(b_i(x))=\operatorname{ord} b_i(x)$$

是$K[[x]]$规定的赋值。又令既约分数

(3) $$\frac{l}{s}=\min\left\{\frac{v(b_i(x))}{i}:i=2,3,\cdots,n\right\}.$$

取$t=x^{1/s}$，$y=t^l z$，代入(2)式，得

$$t^{nl}\left(z^n+\frac{0}{t^l}z^{n-1}+\cdots+\frac{b_i(t^s)}{t^{il}}z^{n-i}+\cdots+\frac{b_n(t^s)}{t^{nl}}\right)=0,$$

即

(4) $g(z)=z^n+c_2(t)z^{n-2}+\cdots+c_n(t)=0$, $c_i(t)=\dfrac{b_i(t^s)}{t^{il}}$.

令$w(c_i(t))=\operatorname{ord}_t c_i(t)$是$K((t))$的赋值，根据(3)式不难看出

$$w(c_i(t))=sv(b_i(x))-il\geqslant 0,\qquad i=2,\cdots,n,$$

而且最少有一个j，使$w(c_j(t))=0$。对(4)式用Hensel引理。在$\bmod tK[[t]]$的意义下，有

(5) $\bar{g}(z)=z^n+c_2(0)z^{n-2}+\cdots+c_n(0)\in K[z]$.

因为K是代数封闭的，又是特征零的，所以(5)式不可能是$(z-a)^n$(否则，$a=0\Longrightarrow c_j(0)=0$，与$w(c_j(t))=0$矛盾；$a\neq 0\Longrightarrow c_1(0)\neq 0$，亦矛盾)。因此(5)式可以分解成两个没有公根的多项

式$\bar{\gamma}(z)$与$\bar{\delta}(z)$的乘积。按照Hensel引理，(4)式也可以分解成

$$g(z)=h(z)q(z).$$

我们只要对次数n取归纳法，便证明了本定理。❙

讨论 1) Hensel引理的要求过强了。事实上，域K不一定要求是完备的，同样也可能有它的结论。最有意义的例子，是K为亚纯函数域$k\{\{x\}\}$(k为特征零的代数封闭域)。因此，同样地，Newton-Puiseux定理对亚纯函数域也是对的，即

$$k\{\{x\}\}\text{的代数闭包}=\bigcup_{n=1}^{\infty}k\{\{x^{1/n}\}\}.$$

2) Newton-Puiseux定理只对K是特征零的情形才是正确的。对K是特征$p\neq 0$的情形是不正确的。例如，下面的多项式在$\bigcup_{n=1}^{\infty}K((x^{1/n}))$中即无解：

$$y^p-y-x^{-1}=0.$$

读者自行检验之。

3) 在第五章中，我们已经证明了域L的代数闭包的存在性。可是那是太抽象了，不够具体。正像我们不能满足于$\boldsymbol{R}$的代数闭包的抽象存在，而要构造出具体的$\boldsymbol{C}$一样，Newton-Puiseux定理也有同样的精神。❙

与定理7.11几乎完全一样地，我们可以证明下面的定理。

定理7.13(Hensel引理) 设R是一个完备的局部环，m是它的极大理想。$\sigma: R\to R/\mathrm{m}$是典型映射，$\sigma(a)=\bar{a}$，$\sigma(f(x))=\bar{f}(x)$($f(x)\in R[x]$)。又设$f(x)$是$R[x]$的首一多项式，$\bar{f}(x)=\gamma(x)\delta(x)$，$\gamma(x)$，$\delta(x)$是$(R/\mathrm{m})[x]$中的首一多项式，$(\gamma(x),\delta(x))=(1)$。那么存在$R[x]$的两个首一多项式$g(x)$，$h(x)$，使

$$f(x)=g(x)h(x),\quad \bar{g}(x)=\gamma(x),\quad \bar{h}(x)=\delta(x).$$

证明 读者仿照定理7.11的证明，自行证之。❙

习　题

1. 证明 $f(x,y)=x^2-y^2-x^3$ 在形式幂级数环 $\boldsymbol{C}[[x,y]]$ 内可以分解。

2. 设 p 是一个素数，$f(x)=x^n+a_1x^{n-1}+\cdots+a_n\in\boldsymbol{Z}[x]$。又令

$$\bar{f}(x)=f(x)(\bmod p).$$

设 $\bar{f}(x)$ 在 $\boldsymbol{Z}/p\boldsymbol{Z}$ 内不可约，试证明 $f(x)$ 在 $\boldsymbol{Q}_p$ 内也不可约。

3. 设 $f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_n\in\boldsymbol{Q}_p[x]$，且不可约。证明：对 $\boldsymbol{Q}_p$ 的赋值 v_p，有

$$\min\{v_p(a_0),v_p(a_1),\cdots,v_p(a_n)\}=\min\{v_p(a_0),v_p(a_n)\}.$$

4. 试将多项式 x^2+1,x^2+2,x^3-3 在 3-adic 数域内进行因式分解。

5. 设域 K 对离散实赋值 v 是完备的，又设

$$f(x)=x^n+a_1x^{n-1}+\cdots+a_n\in K[x].$$

如果 $a_i\in\mathfrak{m}_v(i=1,2,\cdots,n)$，但 a_n 不能表成 $\mathfrak{m}_v$ 内两个元素的乘积，则 $f(x)$ 在 $R_v[x]$ 内不可约。

6. 设 K 对离散实赋值 v 是完备的。令 $R=R_v/\mathfrak{m}_v$。若 $f(x)$ 是 $R_v[x]$ 内首一不可约多项式，证明：$\bar{f}(x)=f(x)(\bmod \mathfrak{m}_v)$ 是 $R[x]$ 内一个不可约多项式的方幂。

7. 证明在 $\boldsymbol{Q}_p$ 内有 $p-1$ 个不同的 $p-1$ 次单位根。

8. 设 R_v 是域 K 的离散赋值环，若 $f(x)\in R_v[x]$ 的某些系数在 R_v 中可逆，则称 $f(x)$ 是本原多项式。证明两个本原多项式的乘积仍是本原多项式。证明 $K[x]$ 内任一非零多项式可以写成 $cg(x)$，其中 $c\neq0$，而 $g(x)$ 是一个本原多项式。如果 $g(x)$ 是 $R_v[x]$ 内本原不可约多项式，试证明：$g(x)$ 在 $K[x]$ 内不可约。

9. 在 $\boldsymbol{Q}_p[x]$ 内分解 x^5-1，此处 $p=3,5,11$，并考虑各因子所引生的域扩充。

10. 设域 K 的特征 $p>0$，证明下列代数方程

$$y^p - y - x^{-1} = 0$$

在 $\bigcup_{n=1}^{+\infty} K((x^{1/n}))$ 中无解。由此导出 $\bigcup_{n=1}^{+\infty} K((x^{1/n}))$ 不是代数封闭域。

11. 设域 K 关于离散赋值 v 是完备域，$R = R_v/\mathfrak{m}_v$。又设 $f(x)$ 是 $R_v[x]$ 内首一多项式。如果 $\bar{f}(x) = f(x) \pmod{\mathfrak{m}_v}$ 在 $R[x]$ 内有一个单重一次因子 $x - \bar{p}$，证明 $f(x)$ 在 $R_v[x]$ 内有一个一次因子 $(x - r)$，且 $\bar{r} = \bar{p}$。

12. 证明方程 $x^3 = 4$ 在 $\mathbf{Q}_5$ 内有根。

§5 代数扩充

设 L 是 K 的代数扩域，v 是 K 的赋值，w_i $(i = 1, \cdots, g)$ 是 v 在 L 的扩充赋值，即 $R_{w_i} \cap K = R_v$，$\mathfrak{m}_{w_i} \cap K = \mathfrak{m}_v$。我们要研究构造 R_{w_i} 的方法，w_i 与 v 的一些数据以及 w_i 的个数等等。

定理7.14 设 L 是 K 的代数扩域，v 是 K 的赋值，w 是 L 的赋值，$R_w \cap K = R_v$，$\mathfrak{m}_w \cap K = \mathfrak{m}_v$。令 S 为 R_v 在 L 中的整数闭包，$\mathfrak{p} = \mathfrak{m}_w \cap S$，那么 $R_w = S_{\mathfrak{p}}$。

证明 根据定理 7.8，$R_w \supset R_v \Longrightarrow R_w \supset S \Longrightarrow R_w \supset S_{\mathfrak{p}}$。反之，任取 $a \in R_w$，a 是对 K 的代数元。令 a 适合下式

(＊) $\quad a_0 a^n + a_1 a^{n-1} + \cdots + a_n = 0, \quad a_i \in K, \ a_0 \neq 0$。

又令 $j = \min\{j:\ v(a_j) \leqslant v(a_i),\ \forall i = 1, 2, \cdots, n\}$。用 a_j 去除(＊)式，得

$$b_0 a^n + b_1 a^{n-1} + \cdots + b_n = 0, \qquad b_j = 1, \ b_i \in R_v.$$

令
$$c = b_0 a^j + b_1 a^{j-1} + \cdots + b_j,$$
$$d = b_{j+1} + b_{j+2} a^{-1} + \cdots + b_n a^{-n+j+1}.$$

则有

$$c a^{n-j} + d a^{n-j-1} = 0, \qquad a = -d/c.$$

我们要说明 $c, d \in S$，$c \notin \mathfrak{p}$。如此就证明了 $a \in S_{\mathfrak{p}}$。

应用定理7.8。任取L的赋值环$R_u \supset S$。如果$a \in R_u$，那么$c \in R_u$，$d = -ac \in R_u$。如果$a \overline{\in} R_u$，那么$a^{-1} \in R_u$，$d \in R_u$，$c = da^{-1} \in R_u$。又因为$b_0, b_1, \cdots, b_{j-1} \in \mathfrak{m}_v \subset \mathfrak{m}_w$，$b_j = 1$，$a \in R_w$，所以$c \overline{\in} \mathfrak{m}_w$，立得$c \overline{\in} \mathfrak{p}$。于是$c$在$S_\mathfrak{p}$中是可逆元，

$$a = -d/c \in S_\mathfrak{p}. \quad \blacksquare$$

系 设L, K, v, R_v, S如上定理，$\mathfrak{p}$为S的一个素理想，那么，$S_\mathfrak{p}$是v的扩充赋值$\Longleftrightarrow \mathfrak{p}$是$S$的极大理想。

证明 $\Longrightarrow$。由于$\mathfrak{p} \cap R_v = \mathfrak{m}_v$，所以$S/\mathfrak{p} \supset R_v/\mathfrak{m}_v$。显然，$S/\mathfrak{p}$对$R_v/\mathfrak{m}_v$是整数相关的。而$R_v/\mathfrak{m}_v$是域，根据第六章§2中的引理，$S/\mathfrak{p}$为域。即$\mathfrak{p}$是$S$的极大理想。

$\Longleftarrow$。根据定理7.6，存在赋值环$R_w \supset S_\mathfrak{p}$，使得$\mathfrak{m}_w \cap S_\mathfrak{p} = \mathfrak{p}S_\mathfrak{p}$。于是不难看出，$R_w \cap K \supset R_v$，$\mathfrak{m}_w \cap K \supset \mathfrak{m}_v$。我们先证明上面的两个包含式都是等式。任取$a \in K \backslash R_v$，那么

$$a^{-1} \in \mathfrak{m}_v \subset \mathfrak{m}_w,$$

得$a \overline{\in} R_w$。又任取$a \in K \backslash \mathfrak{m}_v$，那么$a^{-1} \in R_v \subset R_w$，得$a \overline{\in} \mathfrak{m}_w$。所以$w$是$v$的扩充。而且

$$\mathfrak{m}_w \cap S = \mathfrak{m}_w \cap S_\mathfrak{p} \cap S = \mathfrak{p}S_\mathfrak{p} \cap S = \mathfrak{p},$$

根据上定理，即有$R_w = S_\mathfrak{p}$。 $\blacksquare$

我们定义一个符号：$\Delta_v = R_v/\mathfrak{m}_v$。像以前一样，用$G_v$表示$v$的全序群。当$w$是$v$的扩充时，我们有两个重要的数：一是$[\Delta_w : \Delta_v]$，即$\Delta_w$被考虑成$\Delta_v$上的线性空间时的维数，称为$w$对$v$的**相对次数**(或**剩余次数**)，记为$f(w/v)$(简记为$f$)；二是群指数$[G_w : G_v]$，称为$w$对$v$的**缩分歧指数**，记为$e(w/v)$(简记为$e$)。如果$[G_w : G_v] > 1$，则称$w$是$v$的**分歧性扩充**。

例 13 设$K = \boldsymbol{C}(x)$，$L = \boldsymbol{C}(x)[x^{1/2}] = \boldsymbol{C}(t)$，$t^2 = x$。我们知道$K$的赋值是

$$v_{a^2} \longleftrightarrow \boldsymbol{C}[x]_{(x-a^2)} \text{ 及 } v_\infty \longleftrightarrow \boldsymbol{C}[x^{-1}]_{(x^{-1})}.$$

设$a^2 \neq 0$，那么v_{a^2}的扩充是

$$w_{\pm a} \longleftrightarrow \boldsymbol{C}(t)_{(t \pm a)},$$

这是两个不同的扩充。易见

$$w_a(t-a)=1,\qquad w_a(t+a)=w_a(t-a+2a)=0,$$

$$w_a(x-a^2)=w_a((t-a)(t+a))=1.$$

所以 $G_{w_a}=G_{v_{a^2}}$，$[G_{w_a}:G_{v_{a^2}}]=1$，也即 w_a 是 v_{a^2} 的**非分歧性扩充**。

设$a^2=0$，那么v_0的扩充是$w_0\longleftrightarrow \boldsymbol{C}[t]_{(t)}$，且$w_0(x)=w_0(t^2)=2w_0(t)$。所以，取$G_{w_0}=\boldsymbol{Z}$时，子群$G_{v_0}=2\boldsymbol{Z}$，$[G_{w_0}:G_{v_0}]=2$，所以$w_0$是$v_0$的分歧性扩充，缩分歧指数是2. 同样的，$w_\infty$是$v_\infty$的分歧性扩充，缩分歧指数也是2。参考图7.1(参考复变函数论中的"黎曼曲面")。

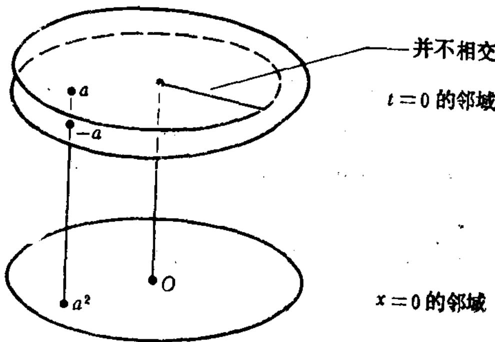


图 7.1

引理1 设$[L:K]=n$，w是v的扩充。那么

1) w对v的相对次数$f\leqslant n$;

2) w对v的缩分歧指数$\leqslant n$。

证明 1) 设$\Delta_w=R_w/\mathrm{m}_w$，$\Delta_v=R_v/\mathrm{m}_v$。又设$\bar{a}$是$a$在典型映射$R_w\to\Delta_w$下的象。我们仅须证明：当$a_1,\cdots,a_l\in R_w$对$K$线性相关时，它们的象$\bar{a}_1,\cdots,\bar{a}_l$必对$\Delta_v$线性相关。设$a_1,\cdots,a_l$适合下面的线性方程

$$b_1a_1+\cdots+b_la_l=0,\qquad b_i\in K,\ b_i\text{不全为零。}$$

令$v(b_j)\leqslant v(b_i)(\forall i=1,\cdots,l)$。以$b_j$去除上式，立得

$$c_1a_1+\cdots+c_la_l=0,\quad c_i\in R_v,\ c_j=1,$$
$$\bar{c}_1\bar{a}_1+\cdots+\bar{c}_l\bar{a}_l=0,\quad \bar{c}_i\in \Delta_v,\ \bar{c}_j=1.$$

2）仅须证明：如果$w(a_1),\cdots,w(a_l)$是属于关于G_v的不同的陪集，那么$a_1,\cdots,a_l$对K线性无关。设有

$$b_1a_1+\cdots+b_la_l=0,\quad b_i\in K,\ b_i\text{不全为零},$$

那么最少有两项$i\neq j$，使$w(b_ia_i)=w(b_ja_j)$，即

$$w(a_i)-w(a_j)=w(b_j)-w(b_i)\in G_v.\ \blacksquare$$

系 $\operatorname{rank} w=1\Longleftrightarrow\operatorname{rank} v=1$。

证明 $\Longrightarrow$。显然。

$\Longleftarrow$。考虑群映射$n':G_w\to G_v\subset \boldsymbol{R}$, $n'(g)=ng$, $\forall g\in G_w$。此处$n=[G_w:G_v]$。$\blacksquare$

引理2 设L是K的有限代数扩域。那么$\operatorname{rank} w=\operatorname{rank} v$。

证明 用定义7.7′。我们需要建立G_w与G_v的孤立子群集合之间的一个单满映射。任取G_w的一个孤立子群H_w，把它对应到$H_v=G_v\cap H_w$。只要证明$H_v\neq G_v$，即不难看出，H_v确是G_v的孤立子群。任取$g\notin H_w$。应用引理1，知

$$[G_w:G_v]=e\leqslant[L:K]<\infty,$$

那么$eg\in G_v$。如果$eg\in H_v$，则$eg\in H_w$。于是$-eg\leqslant g\leqslant eg$或$eg\leqslant g\leqslant -eg$，从而推出$g\in H_w$，与$g$的选取矛盾。因此$H_v\neq G_v$，$H_v$是$G_v$的孤立子群。

反过来，任取G_v的孤立子群H_v，我们把它对应到

$$H_w=\{g\in G_w:\ \text{存在整数}\ s,\ \text{使}\ sg\in H_v\}.$$

不难看出，H_w是G_w的孤立子群。其余的证明请读者补充。$\blacksquare$

引理3 设$[L:K]<\infty$，域L有两个赋值w,w_1，$R_w\subset R_{w_1}\neq L$，$R_v=R_w\cap K$，$R_{v_1}=R_{w_1}\cap K$。它们的全序群分别是G_w，G_{w_1},G_v,G_{v_1}。又如通常一样，设

$\Delta_w=R_w/\mathfrak{m}_w$，$\Delta_{w_1}=R_{w_1}/\mathfrak{m}_{w_1}$，$\Delta_v=R_v/\mathfrak{m}_v$，$\Delta_{v_1}=R_{v_1}/\mathfrak{m}_{v_1}$。

又设 rank $w<\infty$。那么，我们有

1) R_w在Δ_{w_1}中的象定义了一个赋值$\bar{w}_1$，R_v 在 Δ_{v_1}中的象定义了一个赋值 $\bar{v}_1$。$\bar{w}_1$是 $\bar{v}_1$ 的扩充，并且

$$\text{rank } \bar{w}_1<\text{rank } w, \qquad \text{rank } \bar{v}_1<\text{rank } v;$$

2) w 对 v 的相对次数 = $\bar{w}_1$对$\bar{v}_1$的相对次数；

3) w 对 v 的缩分歧指数$[G_w:G_v]=[G_{w_1}:G_{v_1}][G_{\bar{w}_1}:G_{\bar{v}_1}]$.

证明 1) 应用定理7.4，由于 $R_{w_1}\neq L$，所以 $\mathfrak{m}_{w_1}\cap R_w\neq(0)$。因为$R_{\bar{w}_1}=R_w/(\mathfrak{m}_{w_1}\cap R_w)$，而且 R_w 的素理想是互相包含的，自然有

$$\dim R_{\bar{w}_1}<\dim R_w.$$

其余各点都是很容易验证的。

2) 在自然映射下，$\Delta_w\approx\Delta_{\bar{w}_1}$，$\Delta_v\approx\Delta_{\bar{v}_1}$，所以

$$[\Delta_w:\Delta_v]=[\Delta_{\bar{w}_1}:\Delta_{\bar{v}_1}].$$

3) 参见定理7.1后面的两段文字。我们用乘法全序群来代替加法全序群，有

$$G_w=L^*/U_w, \quad G_{w_1}=L^*/U_{w_1},$$
$$G_v=K^*/U_v, \quad G_{v_1}=K^*/U_{v_1},$$
$$G_{\bar{w}_1}=\Delta_{w_1}/U_{\bar{w}_1}, \quad G_{\bar{v}_1}=\Delta_{v_1}/U_{\bar{v}_1},$$

其中U表示赋值环中的可逆元集，例如$U_w=R_w\backslash\mathfrak{m}_w$等等。

显然有 $U_w\cap K^*=U_v$，$U_{w_1}\cap K^*=U_{v_1}$。所以有自然的嵌入

$$G_v\to G_w, \quad G_{v_1}\to G_{w_1}.$$

应用定理7.4，

$$R_{w_1}=(R_w)_{\mathfrak{m}_{w_1}\cap R_w}, \quad R_{v_1}=(R_v)_{\mathfrak{m}_{v_1}\cap R_v},$$

所以，不难看出$U_{w_1}\supset U_w$，$U_{v_1}\supset U_v$。因此，又有一个自然映射的正合序列

$$1\to U_{w_1}/U_w\to G_w\to G_{w_1}\to 1$$

(这无非是说 $G_w/(U_{w_1}/U_w)\approx G_{w_1}$)。考虑自然映射

$$\sigma: U_{w_1}\to\Delta_{w_1}^*$$

不难看出，$\sigma^{-1}(U_{\bar{w}_1})\approx U_w$。而$\sigma$显然是满射，故有

$$U_{w_1}/U_w\approx\Delta^*_{\bar{w}_1}/U_{\bar{w}_1}=G_{\bar{w}_1}.$$

结合上面的正合序列，即有$G_w/G_{\bar{w}_1}\approx G_{w_1}$。类似地，有$G_v/G_{\bar{v}_1}\approx G_{v_1}$。又有

$$G_w\supset G_v,\ G_{w_1}\supset G_{v_1},\ G_{\bar{w}_1}\supset G_{\bar{v}_1},\ G_{\bar{v}_1}=G_v\cap G_{\bar{w}_1},$$

应用群论，得

$$(G_w/G_v)/(G_{\bar{w}_1}/G_{\bar{v}_1})\approx G_{w_1}/G_{v_1}.\ \blacksquare$$

定理7.15 设$n=[L:K]$，v是K的一个有限秩的赋值。又设$w_i(i=1,\cdots,g)$是v在L的扩充，w_i对v的相对次数是f_i，缩分歧指数是e_i。那么，我们恒有

$$e_1f_1+e_2f_2+\cdots+e_gf_g\leqslant n.$$

证明 我们对 rank v 取归纳法。

1) 设rank $v=1$。设$\Delta_i=R_{w_i}/\mathrm{m}_{w_i}$，$\Delta_v=R_v/\mathrm{m}_v$，$G_{w_i}$与$G_v$分别是$w_i$和$v$的全序群。根据引理1的系，rank $w_i=1$。

在G_{w_i}对G_v的每个陪集中分别取一个元素$l_{is}(s=1,\cdots,e_i)$。又在R_{w_i}中取f_i个元素$a_{i1},\cdots,a_{if_i}$，使它们在Δ_{w_i}中的象是对Δ_v线性无关的。

我们要应用定理7.10(逼近定理)。对每个i $(i=1,\cdots,g)$，$s(s=1,\cdots,e_i)$，$t(t=1,\cdots,f_i)$，选取$b_{is},c_{it}\in L$，使之适合下列方程：

$$\begin{aligned}
&w_i(b_{is})=w_i(b_{is}-0)=l_{is},\\
&w_j(b_{is})=w_j(b_{is}-0)(=l)\\
&\qquad\qquad>\max\{l_{is}:\ i=1,\cdots,g,\ s=1,\cdots,e_i\},\qquad j\neq i,\\
&w_i(c_{it}-a_{it})(=\varepsilon_i)>0,\\
&w_j(c_{it})(=\varepsilon_j)>0,\qquad j\neq i.
\end{aligned}$$

只要证明$\{b_{is}\cdot c_{it}\}$是对K线性无关的便足够了(因为这个集合的基数是$e_1f_1+e_2f_2+\cdots+e_gf_g$)。

假设$b_{is}\cdot c_{it}$适合如下的线性方程：

$$\sum_{i,s,t} d_{ist} b_{is} c_{it} = 0, \quad d_{ist} \in K，\text{不全为零.}$$

应用我们多次用过的技巧，不妨令 $d_{111}=1$，$d_{ist} \in R_v$。把上式分成两部分

$$\sum_{s,t} d_{1st} b_{1s} c_{1t} + \sum_{i>1} \sum_{s,t} d_{ist} b_{is} c_{it} = 0.$$

根据b_{is}，c_{it}选取的条件，不难看出

$$w_1(b_{is} c_{it}) > l_{11}, \quad i \geqslant 2,$$

所以 $$w_1\left(\sum_{i>1} \sum_{s,t} d_{ist} b_{is} c_{it}\right) > l_{11}.$$

只要证明下式，便得出了一个矛盾：

$$w_1\left(\sum_{s,t} d_{1st} b_{1s} c_{1t}\right) \leqslant l_{11}.$$

令

$$c_s = \sum_t d_{1st} c_{1t},$$

则

$$\sum_{s,t} d_{1st} b_{1s} c_{1t} = \sum_s c_s b_{1s}.$$

我们将证明

$$w_1(c_s) = \min\{v(d_{1st}):\ t = 1, \cdots, f_n\} \subset G_v.$$

从这里我们就可以得到： (a) $w_1(c_s b_{1s})$属于l_{1s}所在的关于G_v的陪集，因此都不相等。所以

$$w_1\left(\sum_s c_s b_{1s}\right) = \min_s\{w_1(c_s b_{1s})\};$$

(b) $w_1(c_1) = v(d_{111}) = v(1) = 0$，$w_1(c_1 b_{11}) = l_{11}$。于是

$$w_1\left(\sum_s c_s b_{1s}\right) \leqslant l_{11}.$$

综上所述，问题归结为证明下式：

$$w_1(c_s)=\min\{v(d_{1st}):\ t=1,\cdots,f_n\}.$$

设上式右端为$v(d_{1s',t'})$。那么c_s可以改写成

$$c_s=d_{1s',t'}\left(\sum_t d_t^* c_{1t}\right),$$

此处$d_t^*\in R_v$，而且至少有一个$d_t^*=1$。我们只要证明$\sum_t d_t^* c_{1t}$是R_{w_1}的一个可逆元$\left(\text{即}w_1\left(\sum_t d_t^* c_{1t}\right)=0\right)$就足够了。

显然，$w_1(c_{1t}-a_{1t})>0\Longrightarrow \bar{c}_{1t}=\bar{a}_{1t}\in\Delta_{w_1}\Longrightarrow\{\bar{c}_{1t}\}$对$\Delta_v$线性无关$\Longrightarrow\sum_t \bar{d}_t^*\bar{c}_{1t}\neq 0\Longrightarrow\sum_t d_t^* c_{1t}$是$R_{w_1}$的可逆元。

2) 设已知对小于n秩的赋值，本定理是正确的。现设

$$\text{rank } v=n=\text{rank } w_i\qquad(\text{引理 }2).$$

设$\mathfrak{p}_i$是R_{w_i}的仅次于极大理想$\mathfrak{m}_{w_i}$的素理想，易于看出$(R_{w_i})_{\mathfrak{p}_i}$是一个赋值环。令相应的赋值为$w_i'(i=1,\cdots,g)$。设其中不等价的赋值为$w_1',\cdots,w_s'$，它们在$K$上的限制是$v_1,\cdots,v_s$。显然，

$$\text{rank } w_i'=n-1=\text{rank } v_i,$$

所以$R_{v_i}(i=1,\cdots,s)$都是R_v对仅次于极大理想的素理想的局部化环，而这样的素理想是唯一的，于是$v_1=\cdots=v_s$。

令w_i在$\Delta_{w_i'}=R_{w_i'}/\mathfrak{m}_{w_i'}$上定义的赋值为$\bar{w}_i$，$v$在$\Delta_{v_1}$上定义的赋值为$\bar{v}_1$。按照引理3的结论1)，我们知道rank $\bar{v}_1<n$。因此，我们可对v_1及$\bar{v}_1$用归纳法假设，有

$$(1)\qquad\sum_{i=1}^{s}[G_{w_i'}:G_{v_1}][\Delta_{w_i'}:\Delta_{v_1}]\leqslant n.$$

又设$S_i=\{w_j:\ R_{w_j}\subset R_{w_i'}\}\subset\{w_1,\cdots,w_g\}$，那么

$$(2)\qquad\sum_{w_j\in S_i}[G_{\bar{w}_{ji}'}:G_{\bar{v}_1}][\Delta_{\bar{w}_{ji}'}:\Delta_{\bar{v}_1}]\leqslant[\Delta_{w_i'}:\Delta_{v_1}],$$

其中$\bar{w}_{ji}'$是w_j在$\Delta_{w_i'}$上定义的赋值。又根据引理3，

$$[\Delta_{\bar{w}'_{j1}}:\Delta_{\bar{v}_1}]=[\Delta_{w_j}:\Delta_v],$$

$$[G_{w_j}:G_v]=[G_{w'_i}:G_{v_1}][G_{\bar{w}'_{j1}}:G_{\bar{v}_1}].$$

以(2)式代入(1)式后，再将上两式代入，立得

$$\sum_{i=1}^{g}e_if_i\leqslant n. \quad \blacksquare$$

讨论 1) 一般说来，在定理7.15中，既使$w_1,\cdots,w_g$是v的所有的扩充，也不能保证$e_1f_1+e_2f_2+\cdots+e_gf_g=n$。

2) 如果Δ_v的特征是零，那么，取v的所有的扩充$w_1,\cdots,w_g$，则有$e_1f_1+\cdots+e_gf_g=n$。见 Zariski-Samuel 著《Commutative Algebra》，二卷，77页。

例14 设$K=\boldsymbol{R}(x)$，L为$\boldsymbol{R}[x,y]/(x^2+y^2+1)$的比域。可以认为$L\supset K$。如同前面一样的讨论，我们不难看出，$K$的赋值有下面两类：

$$R_v=\boldsymbol{R}[x]_{(h(x))},\qquad h(x)\text{不可约};$$

$$R_v=\boldsymbol{R}[x^{-1}]_{(x^{-1})}.$$

我们知道$\boldsymbol{R}[x]$中的不可约多项式都形如$x-a$或$x^2-2ax+(a^2+b^2)$。以下我们分类讨论。请注意：$[L:K]=2$。

1) $h(x)=x-a$。此时$\Delta_v=R$。令w是v的扩充。立得

$$w(y^2)=v(x^2+1)=0,$$

即 $2w(y)=0$。易于看出

$$\begin{aligned}\Delta_w=\Delta_v(\bar{y})&\approx\boldsymbol{R}[x,y]/(x-a,y^2+x^2+1)\\&\approx\boldsymbol{R}[y]/(y^2+a^2+1),\end{aligned}$$

$$[\Delta_w:\Delta_v]=2.$$

所以根据定理7.15，w是v的唯一的扩充赋值，它的相对次数$f=2$，缩分歧指数$e=1$。

1′) $\boldsymbol{R}[x^{-1}]_{(x^{-1})}$。令$x_1=x^{-1}$，$y_1=x_1y$，经变数替换后，立得$\boldsymbol{R}[x^{-1}]_{(x^{-1})}$与$\boldsymbol{R}[x]_{(x)}$是一样的。

2) $h(x)=x^2+1$，则$2w(y)=w(y^2)=v(x^2+1)$，而$v(x^2+1)$

是v的全序群G_v的生成元。从上式立得

$$e=[G_w:G_v]=2.$$

根据定理7.15，w是v的唯一的扩充赋值，$f=1$，$e=2$。

3) $h(x)$是二次式，$h(x)\neq x^2+1$。即$h(x)=x^2-2ax+(a^2+b^2)$，$b\neq 0$，且当$a=0$时，$b\neq\pm 1$。经过计算，得

$$\begin{aligned}0&=y^2+x^2+1\\&=(y+cx+d)(y-cx-d)+(c^2+1)(x^2-2ax+a^2+b^2),\end{aligned}$$

此处c,d适合下列的联立方程式：

$$\begin{cases}-(c^2+1)a=cd,\\(c^2+1)(a^2+b^2)=d^2+1.\end{cases}$$

在我们的条件下(即$b\neq 0$，当$a=0$时$b\neq\pm 1$)，经过简单计算，可以证明$cx+d\neq 0$。设w是v的一个扩充赋值，那么

$$2w(y)=w(y^2)=v(-x^2-1)\geqslant 0 \implies w(y)\geqslant 0,$$
$$(y+cx+d)(y-cx-d)\in \mathfrak{m}_v\subset \mathfrak{m}_w.$$

所以，$y+cx+d\in \mathfrak{m}_w$或$y-cx-d\in \mathfrak{m}_w$。如果两者都属于$\mathfrak{m}_w$，那么，它们的差$2(cx+d)\in \mathfrak{m}_w$，这是不可能的。不难看出，相应于$(y+cx+d)$及$(y-cx-d)$，有两个$v$的扩充赋值$w_1,w_2$。它们的相对次数$f$都是1(此时$\Delta_v=\boldsymbol{R}[x]/(h(x))\approx\boldsymbol{R}[a+bi]=\boldsymbol{C}$，为代数封闭域，故$\Delta_v$上不能有次数大于1的代数扩张)。它们的缩分歧指数$e$都是1。

请把这个例子与第一章§5“复整数集”对照。1)及1′)相当于那里的惯性型，2)相当于那里的分歧型，3)相当于那里的分解型。▌

现在我们来考虑一秩赋值，即实赋值的情形。我们有下面的定理。

定理7.16 设L是K的有限扩域，$[L:K]=n$，v是K的实赋值，K对v是完备域。那么，v在L上只有一个扩充w，L对w是完备域。

证明 我们先证 L 对 w 是完备域。设 $\{u_1,\cdots,u_n\}$ 是 L 对 K 的一组基。任取 L 的序列 $\{a_i\}$，设

$$a_i=\sum_{j=1}^{n}b_{ij}u_j.$$

我们要说明：$\{a_i\}$ 是 L 对 w 的柯西序列（注意，rank w = rank v $=1$，所以 w 也是实赋值）$\Longleftrightarrow\{b_{ij}\}$ 是对 v 的柯西序列（$\forall j=1,\cdots,n$）。如此，则

$$\lim a_i=\sum(\lim_i b_{ij})u_j\in L,$$

即证明了 L 是完备的。

$\Longleftarrow$。显然。

$\Longrightarrow$。$n=1$ 时，结论是显然的。现在我们用数学归纳法。当 $b_{in}=0(\forall i=1,2,\cdots)$ 时，结论是正确的。假若 $\{a_i\}$ 是 L 的柯西序列，而 $\{b_{in}\}$ 不是 K 的柯西序列，则将导致一矛盾。事实上，此时 $v(b_{in}-b_{jn})\nrightarrow\infty$（注意，距离 $|b_{in}-b_{jn}|=\exp(-v(b_{in}-b_{jn}))$）。那么，存在一个 l，及一序列的整数对 (p_i,q_i)，使 $p_i,q_i\to\infty$，而且

$$v(b_{p_in}-b_{q_in})<l.$$

令

$$c_i=\frac{a_{p_i}-a_{q_i}}{b_{p_in}-b_{q_in}}=d_{i1}u_1+\cdots+d_{i,n-1}u_{n-1}+u_n,$$

则

$$w(c_i)=w(a_{p_i}-a_{q_i})-v(b_{p_in}-b_{q_in})\to\infty.$$

所以 $\{c_i-u_n\}$ 是一个柯西序列，并且适合归纳法前提的要求，因此 $\{d_{ij}\}(j=1,\cdots,n-1)$ 是 K 的柯西序列。取极限后，得

$$\begin{aligned}0=\lim c_i&=(\lim d_{i1})u_1+\cdots+(\lim d_{i,n-1})u_{i-1}+u_n\\&=d_1u_1+\cdots+d_{n-1}u_{n-1}+u_n,\qquad d_i\in K,\end{aligned}$$

它与 $\{u_1,\cdots,u_n\}$ 是 L 对 K 的一组基的已知条件不合。这就是我们

要导出的矛盾。

现在证明 w 的唯一性。设 w_1 与 w_2 是 v 的两个扩充。那么，任取 L 的序列 $\{a_i\}$，我们有

$$\lim w_1(a_i)=\infty \iff \lim a_i=0 \iff \lim w_2(a_i)=\infty.$$

设 $a\in \mathfrak{m}_{w_1}$，那么

$$\lim w_1(a^i)=\infty \implies \lim w_2(a^i)=\infty \implies w_2(a)>0$$
$$\implies a\in \mathfrak{m}_{w_2}.$$

所以 $\mathfrak{m}_{w_1}\subset \mathfrak{m}_{w_2}$。同样可证 $\mathfrak{m}_{w_2}\subset \mathfrak{m}_{w_1}$。所以 $\mathfrak{m}_{w_2}=\mathfrak{m}_{w_1}$。若 $a\in R_{w_1}\backslash \mathfrak{m}_{w_1}$，显然 $a^{-1}\overline{\in} \mathfrak{m}_{w_1}=\mathfrak{m}_{w_2}$，故 $a\in R_{w_2}$。所以 $R_{w_1}\subset R_{w_2}$。同法可证 $R_{w_2}\subset R_{w_1}$。于是 $R_{w_1}=R_{w_2}$，即 $w_1=w_2$。 ∎

讨论 事实上，$w(a)=v(\mathrm{N}_{L/K}(a))/n$。参看定义5.16。

定理7.17 设 L 是 K 的有限可离代数扩域，$[L:K]=n$。设 v 是 K 的一个实赋值，$w_1,\cdots,w_g$ 是 v 在 L 上的所有的扩充。设 $\hat{L}_i$ 是 L 对 w_i 的完备化域，$\hat{K}$ 是 K 对 v 的完备化域，$n_i=[\hat{L}_i:\hat{K}_i]$。那么，我们恒有

$$n=\sum_{i=1}^{g} n_i.$$

证明 设 $L=K[a]\approx K[x]/(f(x))$。又设 $f(x)$ 在 $\hat{K}[x]$ 中分解为首一的不可约多项式的乘积如下：

$$f(x)=\prod_i f_i(x).$$

取定 $\hat{K}$ 的一个代数闭包 Ω。对 L 的任一赋值 w_i，其相应的完备域 $\hat{L}_i$ 是 $\hat{K}$ 的代数扩张，故存在由 $\hat{L}_i$ 到 Ω 的 $\hat{K}$ 嵌射(即保持 $\hat{K}$ 不动的嵌射) σ_i。K 的赋值 v 可以自然地扩充为 $\hat{K}$ 的赋值，仍记为 v。根据上定理，v 在 $\sigma_i(\hat{L}_i)$ 中有唯一的扩充 w_i^*。容易看出，映射

$$w_i':\ \hat{L}_i\to \boldsymbol{R},$$
$$w_i'(a)=w_i^*(\sigma_i(a))$$

是 $\hat{L}_i$ 的一个赋值，而且是 $\hat{K}$ 的赋值 v 的扩充。根据上定理，即知

$w_i = w'_i$。按照同样的道理，易知

$$w_j \neq w_i \Longrightarrow \sigma_j(\hat{L}_j) \not\approx \sigma_i(\hat{L}_i),$$

这里的同构是指$\hat{K}$同构。

易知$\sigma_i(\hat{L}_i) = \sigma_i(L) \cdot \hat{K} = \hat{K}[\sigma_i(a)]$。$\sigma_i(a)$显然是 $f(x)$的某个因子$f_{l(i)}(x)$的根。而且不难看出，当$i \neq j$时，必有

$$f_{l(i)}(x) \neq f_{l(j)}(x).$$

事实上，否则

$$\sigma_i(\hat{L}_i) \approx \hat{K}[x]/(f_{l(i)}(x)) = \hat{K}[x]/(f_{l(j)}(x)) \approx \sigma_j(\hat{L}_j),$$

与上面的结果矛盾。这样，我们就建立了由$\{w_1, \cdots, w_g\}$到$\{f_1(x), f_2(x), \cdots\}$的一个单射。

反之，任取$f_l(x)$，视$\hat{K}[x]/(f_l(x))$为 Ω的子域，我们可以作由L到Ω的K嵌射σ，使

$$\sigma(a) = \bar{x} \in \hat{K}[x]/(f_l(x)) \subset \Omega.$$

$\hat{K}$的赋值v在$\hat{K}[x]/(f_l(x))$上有唯一的扩充w，w在$\sigma(L)$上的限制唯一决定了L的一个赋值w_i。于是，我们上面所建立的由$\{w_1, \cdots, w_g\}$到$\{f_1(x), f_2(x), \cdots\}$的单射也是满射。所以

$$n = [L:K] = \deg f(x) = \sum_i \deg f_i(x)$$

$$= \sum_i [\hat{L}_i : \hat{K}] = \sum_i n_i. \quad \blacksquare$$

讨论 本定理中的$\hat{K}$及$\hat{L}_i$都称为**局部域**，L, K称为**整体域**，$[L:K]$称为**整体次数**，$[\hat{L}_i:\hat{K}]$称为**局部次数**。上面的定理又可以叙述为

$$\text{整体次数} = \sum \text{局部次数}.$$

例 15 令

$$L = \mathbf{Q}[a] \approx \mathbf{Q}[x]/(x^3+2), \quad K = \mathbf{Q}, \quad R_v = \mathbf{Z}_{(3)}, \quad \hat{K} = \mathbf{Q}_3.$$

应用Hensel引理，因为

$$x^3 + \bar{2} = (x - \bar{1})(x^2 + \bar{1} \cdot x - \bar{2}) \in \mathbf{Z}/3\mathbf{Z}[x],$$

所以

$$x^3+2=(x-(1+\cdots))(x^2+(1+\cdots)x-(2+\cdots))$$
$$=(x-\alpha)(x^2+\alpha x-\beta)\in \mathbf{Q}_3[x].$$

因此，R_v在L中有两个扩充，一个是由映射$L\to\mathbf{Q}_3$，$a\mapsto\alpha$所引生的，另一个是由映射$L\to\mathbf{Q}_3[x]/(x^2+\alpha x-\beta)$，$a\mapsto\bar{x}$所引生的。我们有

$$\text{整体次数}=3=\sum\text{局部次数}=1+2.$$

定理 7.18 设L是K的有限扩域，$[L:K]=n$，v是K的一秩离散赋值(即$G_v\approx \mathbf{Z}$)，K对v是完备域，w是v在L中的唯一扩充。那么，$ef=n$。

证明 令$\mathfrak{m}_v=(t)$，$\mathfrak{m}_w=(\tau)$，$t=a\tau^e$，其中a为R_w的可逆元。在L中取$a_1,\cdots,a_f$，使它们在Δ_w中的象是对Δ_v线性无关的。我们只要证明

$$\{a_i\tau^j:\ i=1,\cdots,f,\ j=0,\cdots,e-1\}$$

是L对K的生成元集，便得出$ef\geqslant n$。结合定理7.15，立得本定理。

任取$b\in L$。显然，当$s\to\infty$时，

$$w(t^s b)=sw(t)+w(b)=se+w(b)\to\infty.$$

这就是说，当s充分大时，$t^s b\in R_w$。因此，我们只要对于$b\in R_w$，证明b可以写成下列的线性式便足够了：

$$b=\sum_{i,j}c_{ij}a_i\tau^j,\qquad c_{ij}\in R_v.$$

令σ：$R_w\to R_w/\mathfrak{m}_w$是典型映射，那么根据$\{a_i\}$的选取，

$$\sigma(b)=\sum_i \bar{c}_{i0}^{(0)}\sigma(a_i),\ \bar{c}_{i0}^{(0)}\in\Delta_v.$$

取$c_{i0}\in R_v$，使$\sigma(c_{i0}^{(0)})=\bar{c}_{i0}^{(0)}$，即有

$$b-\sum_i c_{i0}^{(0)}a_i\in(\tau).$$

同法考虑$\left(b-\sum_i c_{i0}^{(0)}a_i\right)\tau^{-1}$，得

$$b-\sum_i c_{i0}^{(0)}a_i-\sum_i c_{i1}^{(0)}a_i\tau\in(\tau^2).$$

不难依次作下去。当我们必须用τ^e时，利用 $t=a\tau^e$，$\tau^e=a^{-1}t$，以$a^{-1}t$取代τ^e。经过整理，不难得出

$$b=\sum_{i,j}\left(\sum_{l=0}^{\infty}c_{ij}^{(l)}\right)a_i\tau^j=\sum_{i,j}c_{ij}a_i\tau^j. \quad \blacksquare$$

例 16 设k,k'是域，$k'((\tau))\supset k((t))$，其中 t 为变数，$[k'(\tau):k(t)]=n$。那么，$t=a\tau^e$，a 为$k'[[\tau]]$的可逆元，$k'=R_w/\mathfrak{m}_w$，$k=R_v/\mathfrak{m}_v$，$f=[k':k]$。

定理7.19 设L是K的有限可离代数扩域，v是K的一秩离散赋值，$w_1,\cdots,w_g$是v在L上的所有的扩充，w_i对v的相对次数是f_i，缩分歧指数是e_i。那么

$$\sum_i e_i f_i=n.$$

证明 根据定理7.17，$\sum_i n_i=n$，这里$n_i=[\hat{L}_i:\hat{K}]$，$\hat{L}_i$与$\hat{K}$是L(对w_i)及K(对v)的完备化域。根据定理7.9，在完备化作用下，全序群G_{w_i},G_v，剩余域Δ_{w_i},Δ_v皆不变，因此相对次数f_i及缩分歧指数e_i也皆不变。根据定理7.18，即有$n_i=e_if_i$。所以立得

$$\sum_i e_if_i=\sum_i n_i=n. \quad \blacksquare$$

习　题

1. 在 p-adic 数域 $\boldsymbol{Q}_p$ 内确定其赋值的值群、赋值环和赋值环的极大理想，证明其剩余域同构于 $\boldsymbol{Z}/p\boldsymbol{Z}$。

2. 试决定 $\boldsymbol{Q}(\mathrm{i})$ 内的赋值，使它们是 $\boldsymbol{Q}$ 内 7-adic 赋值的扩充。

3. 试决定 $\boldsymbol{Q}(\mathrm{i})$ 的所有可能的赋值。

4. 设 L, L' 是域 K 的两个有限次扩域，且 L 到 L' 存在一个保持 K 的元素不动的同构 σ。又设 K 内赋值 v 在 L' 有一扩充 w'。证明

$$w(x) = w'(\sigma(x)) \quad (x \in L)$$

是 L 的一个赋值，且为 v 的一个扩充。

5. 设 K 是 p-adic 数域 $\boldsymbol{Q}_p$ 的有限次扩域，α, β 是 $\boldsymbol{Q}_p$ 上不可约多项式 $f(x)$ 在 K 内的两个根，又设 $\boldsymbol{Q}_p$ 内赋值 v 在 K 上扩充为 w，证明：$w(\alpha) = w(\beta)$。

6. 设 K 是 $\boldsymbol{Q}$ 的伽罗瓦扩域，证明 $\boldsymbol{Q}$ 内赋值 v 在 K 的任意两个扩充 w_1, w_2 都有相同的相对次数和缩分歧指数。

7. 设 K 是域，v 是 K 上一秩离散赋值。证明 v 的剩余域 $R_v/\mathfrak{m}_v$ 与 K 特征相同的充分必要条件是：R_v 包含 K 的素域。

8. 设 K 关于离散赋值 v 是完备域，L 是 K 的有限次扩域，v 在 L 内的扩充记为 w。如果 w 对 v 的缩分歧指数等于 $[L:K]$，则称扩充 L/K 是**全分歧的**。现令 π, p 分别为 $\mathfrak{m}_w, \mathfrak{m}_v$ 的生成元。证明 L/K 全分歧的充要条件是：π 满足方程

$$x^n + a_1 p x^{n-1} + \cdots + a_{n-1} p x + a_n p = 0,$$

其中 $a_i \in K$，$v(a_i) \geqslant 0$，$v(a_n) = 0$，$n = [L:K]$，$L = K(\pi)$。

9. 设 K 是完备域，证明 K 的赋值可唯一地扩充为它的代数闭包 $\bar{K}$ 的赋值。

10. 证明 p-adic 数域 $\boldsymbol{Q}_p$ 的代数闭包 $\bar{\boldsymbol{Q}}_p$ 不是完备的。

11. 令 $\zeta = \exp(2\pi\mathrm{i}/5)$，$K = \boldsymbol{Q}(\zeta)$，试求 $\boldsymbol{Q}$ 的 p-adic 赋值在

K内互不等价的扩充的个数，此处$p=3,5,11$。

§6 因子类群

关于赋值论在代数数论中的应用，请见下一章“Dedekind整环”。我们在本节里，讨论赋值论在代数几何学中的应用。

设k是一个域，或称为“数域”。我们常常假设k是代数封闭的(参考第六章的希尔伯特零点定理)，$K=k(x_1,\cdots,x_r)$，此处$x_1,\cdots,x_r$不一定是代数无关的。K称为**代数函数域**。设

$$\operatorname{tr}\deg(K/k)=n.$$

定义7.9 设v是K的k赋值。如果$\operatorname{tr}\deg(\Delta_v/k)=n-1$，则称$v$是$K$的**素因子**。

讨论 根据定理7.5，$\operatorname{rank} v+\operatorname{res-dim} v\leqslant n$。请注意，

$$\operatorname{res-dim} v=\operatorname{tr}\deg(\Delta_v/k),$$

因此$\operatorname{rank} v\leqslant 1$。又知$\operatorname{rank} v\neq 0$，所以$\operatorname{rank} v=1$。

例17 设$K=k(x_1,\cdots,x_n)$，$\operatorname{tr}\deg(K/k)=n$，$v$是$K$的素因子。如果$v(x_i)<0$，则用$x_i^{-1}$取代$x_i$，即不妨设$v(x_i)\geqslant 0$ ($\forall i=1,2,\cdots,n$)。所以$R_v\supset k[x_1,\cdots,x_n]$。我们要说明，当

$$\operatorname{tr}\deg((k[x_1,\cdots,x_n]/\mathfrak{p})/k)=n-1$$

时，$\operatorname{ht}(\mathfrak{p})=1$，此处$\mathfrak{p}=\mathfrak{m}_v\cap k[x_1,\cdots,x_n]$。

假设有$(0)\subsetneqq\mathfrak{p}_1\subsetneqq\mathfrak{p}$，此处$\mathfrak{p}_1$是一个素理想。令

$$S=k[x_1,\cdots,x_n]/\mathfrak{p}_1=k[\bar{x}_1,\cdots,\bar{x}_n],\quad \bar{\mathfrak{p}}=\mathfrak{p}/\mathfrak{p}_1.$$

那么，$\operatorname{tr}\deg(S/k)<n$。用诺德正规化定理，存在$S_1=k[y_1,\cdots,y_r]$，$y_1,\cdots,y_r$是代数无关的，$S$对$S_1$是整数相关的。不难看出，$\bar{\mathfrak{p}}\cap S_1\neq(0)$，

$$\operatorname{tr}\deg((S/\bar{\mathfrak{p}})/k)=\operatorname{tr}\deg((S_1/\bar{\mathfrak{p}}\cap S_1)/k)\leqslant n-2,$$

而且$k[x_1,\cdots,x_n]/\mathfrak{p}=S/\bar{\mathfrak{p}}$，$\Delta_v$是$k[x_1,\cdots,x_n]/\mathfrak{p}$的比域。因此得到一个与前提相矛盾的结论：$\operatorname{tr}\deg(\Delta_v/k)\leqslant n-2$。所以我们知道$\operatorname{ht}(\mathfrak{p})=1$。

任取$f\in\mathfrak{p}$，设f的素因子分解式为$f=\prod_i f_i$。因为$\mathfrak{p}$是素理想，所以必有一个$f_i\in\mathfrak{p}$。但是(f_i)也是一个素理想，且$\mathrm{ht}(\mathfrak{p})=1$，所以$(f_i)=\mathfrak{p}$。这就说明了在一个唯一分解的整环里，$\mathrm{ht}(\mathfrak{p})=1\Longrightarrow\mathfrak{p}$是主理想。

显然，$k[x_1,\cdots,x_n]_{(f_i)}$是一个一秩离散赋值环，而且它含于$R_v$中。因此，我们得出$R_v=k[x_1,\cdots,x_n]_{(f_i)}$。

从几何与代数的联系来看，在$k[x_1,\cdots,x_n]$上有限的而且

$$\mathrm{tr\,deg}((k[x_1,\cdots,x_n]/\mathfrak{p})/k)=n-1$$

的素因子，相当于A^n中由$f_i=0$定义的$n-1$维不可分解的代数多样体。

定理7.20 K的素因子v必然是一秩离散赋值。

证明 仅须证明v是离散的(参看上面的讨论)。取$x_1,\cdots,x_{n-1}$，使它们在Δ_v中的象对k是代数无关的。又取x_n，使$x_1,\cdots,x_n$对k是代数无关的，以及$v(x_n)\geqslant 0$（如果$v(x_n)<0$，就用x_n^{-1}取代x_n）。令$S=k[x_1,\cdots,x_n]$，它的比域为$K_1=k(x_1,\cdots,x_n)$，u是v在K_1上的限制。

因为K是K_1的代数扩域，所以$\mathrm{rank}\,u=\mathrm{rank}\,v=1$。由于

$$[\Delta_v:\Delta_u]\geqslant[K:K_1],$$

所以Δ_v是Δ_u的代数扩域，即有

$$\mathrm{tr\,deg}(\Delta_u/k)=\mathrm{tr\,deg}(\Delta_v/k)=n-1,$$

于是u是K_1的素因子。

我们要说明$\mathrm{tr\,deg}((S/\mathfrak{p})/k)=n-1$，这里$\mathfrak{p}=\mathfrak{m}_u\cap S$。显然，

$$S/\mathfrak{p}=k[\bar{x}_1,\cdots,\bar{x}_n]\subset\Delta_v,$$

已经知道其中的$\bar{x}_1,\cdots,\bar{x}_{n-1}$是代数无关的。假若$\bar{x}_1,\cdots,\bar{x}_n$是代数无关的，那么，$S\to S/\mathfrak{p}$是单满映射，于是

$$\mathfrak{p}=(0),\quad R_u\supset S_{(0)}=K_1,\quad \mathrm{rank}\,u=0.$$

这与$\mathrm{rank}\,u=1$不合。

根据例17的讨论，u是一秩离散赋值。又根据§5中定理

7.15的引理1，存在整数s，使$sG_v \subset G_u \approx \boldsymbol{Z}$，不难导出

$$G_v \approx \boldsymbol{Z}. \ \blacksquare$$

系 设v是K的素因子，那么，R_v是一维的正则诺德局部环。

证明 应用定理7.3的2)。▌

讨论 一秩离散赋值v不一定是素因子。请看下面的例子。

例18 令$\sigma(x)=t$，$\sigma(y)=e^t$。由于t及e^t是代数无关的，所以σ：$\boldsymbol{C}(x,y)\to\boldsymbol{C}((t))$是域的嵌射。又令$w$是$\boldsymbol{C}((t))$的赋值：

$$w(f(t))=\mathrm{ord}_t f(t), \quad f(t)\in\boldsymbol{C}((t)).$$

v是w在$\boldsymbol{C}(x,y)$上的限制。显然

$$G_v \subset G_w \approx \boldsymbol{Z},$$

所以，v是一秩离散赋值。但是

$$\boldsymbol{C} \subset \Delta_v \subset \Delta_w = \boldsymbol{C},$$

即$\mathrm{tr\,deg}(\Delta_v/\boldsymbol{C})=0$，所以$v$不是一个素因子。

例19 设v是$K=k(x_1,\cdots,x_r)$的素因子，$\mathfrak{p}=\mathfrak{m}_v\cap k[x_1,\cdots,x_r]$。那么，$\mathrm{tr\,deg}((k[x_1,\cdots,x_r]/\mathfrak{p})/k)$不一定等于$n-1$，这里$n=\mathrm{tr\,deg}(K/k)$。因此不一定合于例17的讨论。现在我们举一个与例17不同的例子。

设$K=k[x_1,x_2]$，$\mathrm{tr\,deg}(K/k)=2$。令$v=\mathrm{ord}$，即，如果$f(x_1,x_2)$与$g(x_1,x_2)\in k[x_1,x_2]$，则令

$$v(f(x_1,x_2))=f(x_1,x_2)\text{的最低次数},$$

$$v(f(x_1,x_2)/g(x_1,x_2))=v(f(x_1,x_2))-v(g(x_1,x_2)).$$

事实上，此时$R_v=k[x_1,x_2/x_1]_{(x_1)}$，$G_v\approx\boldsymbol{Z}$，$\Delta_v\approx k(x_2/x_1)$。所以$v$是$K$的素因子。可是

$$\mathfrak{p}=\mathfrak{m}_v\cap k[x_1,x_2]=(x_1,x_2),$$

即$\mathrm{tr\,deg}((k[x_1,x_2]/\mathfrak{p})/k)=0<1$。这也就是说，$\mathrm{ht}(\mathfrak{m}_v\cap k[x_1,x_2])=2>1$，$v$在$k[x_1,x_2]$上的中心是$(x_1,x_2)$，相当于几何学的一点。▌

考虑例17以及例19，我们给出下面的定义。

定义7.10 设有整环$S=k[x_1,\cdots,x_r]$，K是它的比域。又设v是K的素因子，$\mathfrak{p}=\mathfrak{m}_v\cap S$。如果

$$\operatorname{tr}\deg((S/\mathfrak{p})/k)=\operatorname{tr}\deg(\Delta_v/k)=n-1,$$

那么，称v为对S的**第一类素因子**。否则称v为对S的**第二类素因子**。

我们先证明下面的引理。

引理1 设有整环$S=k[x_1,\cdots,x_r]$，K是它的比域。那么，对素理想$\mathfrak{p}$而言，

$$\operatorname{tr}\deg((S/\mathfrak{p})/k)=\operatorname{tr}\deg(K/k)-1=n-1\Longleftrightarrow \operatorname{ht}(\mathfrak{p})=1.$$

证明 用诺德正规化定理，选取$y_1,\cdots,y_n$，使$y_1,\cdots,y_n$对k是代数无关的，而且S是对$S_1=k[y_1,\cdots,y_n]$整数相关的。令$\mathfrak{p}_1=\mathfrak{p}\cap S_1$。不难看出，

$$\operatorname{ht}(\mathfrak{p})=\operatorname{ht}(\mathfrak{p}_1)\quad（为什么？）,$$

$$\operatorname{tr}\deg((S/\mathfrak{p})/k)=\operatorname{tr}\deg((S_1/\mathfrak{p}_1)/k).$$

因此，本引理简化成$S_1,\mathfrak{p}_1$的情形了。

$\Longleftarrow$。因为S_1是唯一分解整环，所以$\mathfrak{p}_1=(f)$，f是不可分解的多项式（参看例17）；$f\neq 1,0$。于是，不难看出，

$$\operatorname{tr}\deg((S_1/\mathfrak{p}_1)/k)=n-1.$$

$\Longrightarrow$。设有素理想$\mathfrak{p}_2$，使$0\subsetneqq\mathfrak{p}_2\subsetneqq\mathfrak{p}_1$。那么，令$S_2=S_1/\mathfrak{p}_2$，则$\operatorname{tr}\deg(S_2/k)\leqslant n-1$。易见

$$S_1/\mathfrak{p}_1\approx S_2/(\mathfrak{p}_1/\mathfrak{p}_2),\qquad \operatorname{ht}(\mathfrak{p}_1/\mathfrak{p}_2)\leqslant 1,$$

所以，同理得出

$$\operatorname{tr}\deg((S_1/\mathfrak{p}_1)/k)\leqslant\operatorname{tr}\deg(S_2/k)-1\leqslant n-2,$$

这与已知条件不合。▌

讨论 根据引理，$k[x_1,\cdots,x_r]$的任意一个不能加长的素理想链$(0)\subsetneqq\mathfrak{p}_1\subsetneqq\mathfrak{p}_2\subsetneqq\cdots\subsetneqq\mathfrak{p}_l$，必定有长度$n$。同理可以看出，两个素理想$\mathfrak{p}\subset\mathfrak{q}$之间的不能加长的素理想链$\mathfrak{p}\subsetneqq\mathfrak{q}_1\subsetneqq\cdots\subsetneqq\mathfrak{q}_t\subsetneqq\mathfrak{q}$必有相同的长度。我们称这种性质为**垂链性**。上文说明了$k[x_1,\cdots,x_r]$有垂链性。

定义7.10′ 如果$\text{ht}(\mathfrak{m}_v \cap S)=1$，则称$v$是对$S$的**第一类素因子**，此处$v, S$等是与定义7.10一样的。

讨论 考虑满射

$$\sigma: k[X_1,\cdots,X_r] \twoheadrightarrow k[x_1,\cdots,x_r]=S,$$

$\sigma(X_i)=x_i$，这里$X_1,\cdots,X_r$是变数。$\mathfrak{q}=\sigma^{-1}(0)$是$k[X_1,\cdots,X_r]$的一素理想，$\mathscr{V}(\mathfrak{q})$是$r$维仿射空间$\mathbf{A}^r$中的一代数多样体$V$，$k[x_1,\cdots,x_r]$是$V$上的多项式函数环。设$\mathfrak{p}$是$k[x_1,\cdots,x_r]$的一素理想，令$\sigma^{-1}(\mathfrak{p})=\mathfrak{q}_1$，则$\mathscr{V}(\mathfrak{q}_1)=W$是$V$的一子代数多样体。此时有

$$\text{ht}(\mathfrak{p})=1 \Longleftrightarrow \dim W=\dim V-1$$

（见上面的引理）。于是，v是对S的第一类素因子$\Longleftrightarrow v$在S的中心$\mathfrak{p}$相应于一个$n-1$维的不可分解的子多样体。一般言之，$v \twoheadrightarrow \mathfrak{p}$的对应不是单射（请看下面的解说）。▌

我们要讨论整数封闭的环S。整数封闭的环也称为**正规环**。有下面的定理。

定理7.21 一个一维诺德正规局部整环S必定是它的比域K的一个一秩离散赋值环。

证明 根据定理7.3，仅须证明S是一个正则环便足够了。这就是说，我们仅须证明S的极大理想$\mathfrak{m}$是一个主理想。以下分段说明。

1）令$\mathfrak{m}^{-1}=\{b\in K: b\mathfrak{m}\subset S\}$。显然，$\mathfrak{m}^{-1}$是一个$S$模，

$$\mathfrak{m}^{-1}\supset S, \quad \mathfrak{m}\subset\mathfrak{m}\mathfrak{m}^{-1}\subset S.$$

不难看出，$\mathfrak{m}\mathfrak{m}^{-1}$是$S$的一个理想，所以$\mathfrak{m}\mathfrak{m}^{-1}=\mathfrak{m}$或$S$。

我们先证明$\mathfrak{m}^{-1}\neq S$：任取$a\in\mathfrak{m}$，$a\neq 0$，考虑理想(a)的简略准素分解，因为S只有一个非零的素理想$\mathfrak{m}$，所以(a)是一准素理想，$\mathfrak{m}$是它的相伴素理想。因此存在$c\in S$，使$\mathfrak{m}=((a):c)$（见定理6.21的证明）。显然$c\notin(a)$（否则$((a):c)=S\neq\mathfrak{m}$），所以$c/a\notin S$，$c/a\in\mathfrak{m}^{-1}$，因此$\mathfrak{m}^{-1}\supsetneqq S$。

2）证明$\mathfrak{m}\mathfrak{m}^{-1}=S$。假若不然，则$\mathfrak{m}\mathfrak{m}^{-1}=\mathfrak{m}$，任取$a\in\mathfrak{m}^{-1}$，则$a\mathfrak{m}\subset\mathfrak{m}$。令$\mathfrak{m}=(b_1,\cdots,b_l)$，那么

$$ab_i = \sum_{j=1}^{l} c_{ij} b_j, \qquad c_{ij} \in S(i=1,\cdots,l).$$

于是令

$$\det\begin{bmatrix} a-c_{11} & -c_{12} & \cdots\cdots & -c_{1l} \\ -c_{21} & a-c_{22} & \cdots\cdots & -c_{2l} \\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots \\ -c_{l1} & -c_{l2} & \cdots\cdots & a-c_{ll} \end{bmatrix} = a^l + c_1 a^{l-1} + \cdots + c_l = \lambda,$$

即有 $\lambda\mathfrak{m}=(0)$（参见定理6.6的证明）。所以 $\lambda=0$，也即 a 对 S 是整数相关的。已知 S 是正规环，立得 $\mathfrak{m}^{-1}\subset S$，这与 1）相冲突。因此 $\mathfrak{m}\mathfrak{m}^{-1}=S$。

3）根据定理6.35，我们有 $\bigcap\mathfrak{m}^i=(0)$。所以 $\mathfrak{m}\neq\mathfrak{m}^2$。任取 $a\in\mathfrak{m}\backslash\mathfrak{m}^2$。不难看出 $a\mathfrak{m}^{-1}$ 是 S 的理想。我们要说明 $a\mathfrak{m}^{-1}=S$。假若不然，$a\mathfrak{m}^{-1}\subset\mathfrak{m}$，那么，$a\in a\mathfrak{m}^{-1}\mathfrak{m}\subset\mathfrak{m}^2$，与 a 的选取不合。因此 $a\mathfrak{m}^{-1}=S$。于是立得

$$(a)=aS=a\mathfrak{m}^{-1}\mathfrak{m}=S\mathfrak{m}=\mathfrak{m},$$

即 $\mathfrak{m}$ 是主理想。▎

讨论 1）设 $S=k[x_1,\cdots,x_r]$ 是诺德正规整环，K 是它的比域。设 v 是对 S 的第一类素因子。令 $\mathfrak{m}_v\cap S=\mathfrak{p}$，则有 $\mathrm{ht}(\mathfrak{p})=1$，$S_\mathfrak{p}$ 是一维诺德正规局部环，因此是一个一秩离散赋值环。自然 $R_v\supset S_\mathfrak{p}$，$\mathrm{rank}\, R_v=\mathrm{rank}\, S_\mathfrak{p}$。应用定理7.4，立得 $R_v=S_\mathfrak{p}$。因此，对 S 的第一类素因子 v 的赋值环，即是 S 对高度为1的素理想的局部化环。

2）从几何的观点来看，当 $S=k[x_1,\cdots,x_n]$ 是正规整环时，对 S 的第一类素因子 v 即相当于代数多样体 V 的 $n-1$ 维子代数多样体 W，此处 S 是 V 的多项式函数环，$n=\dim V$。

例20 取 $S=k[t^2,t^3]$，则 S 不是一个正规环。这是因为 $t\in K$（K 为 S 的比域），$t^2\in S$，$t\notin S$。令 $\mathfrak{p}=(t^2,t^3)$，不难看出，$\mathrm{ht}(\mathfrak{p})=1$，但 $S_\mathfrak{p}$ 不是正规环，因此 $S_\mathfrak{p}$ 也不是一个赋值环。▎

设V是n维不可分解的**正规代数多样体**，这就是说，它的多项式函数环$S=k[x_1,\cdots,x_r]$是正规的，而且$\dim S=n$。我们引入它的所有的$n-1$维不可分解的子代数多样体W_i所生成的自由交换群$D(V)$（也记为$D(S)$），即

$$D(V)=\left\{\sum_{\text{有限}}n_iW_i:\ n_i\in \boldsymbol{Z},\ W_i\text{ 是 }V\text{ 的 }n-1\text{ 维不可分解的子代数多样体}\right\}.$$

这个群$D(V)$称为V的**因子群**，其元素称为**因子**。

任取$f\in S$，考虑理想(f)。我们要说明：包含(f)的高度为1的素理想$\mathfrak{p}$只有有限多个。这是因为，考虑(f)的简略准素分解以后，不难得出，$\mathfrak{p}$必然是(f)的一个孤立素理想。以v_w表示与$n-1$维子多样体W相对应的赋值，那么

$$v_w(f)>0 \iff (f)\subset\mathfrak{p},\ \mathfrak{p}=\mathfrak{m}_{v_w}\cap S.$$

因此，任取$h=f/g\in K$（K表示S的比域），定义

$$(h)=\sum v_w(h)W.$$

则只有有限多个$v_w(h)\neq 0$，所以$(h)\in D(V)$。这样定义的h的因子(h)称为**主因子**。显然，我们有

$$\begin{aligned}(h_1h_2)&=\sum v_w(h_1h_2)W=\sum v_w(h_1)W+\sum v_w(h_2)W\\&=(h_1)+(h_2).\end{aligned}$$

因此，所有的主因子形成$D(S)$的一个子群$F(S)$。商群

$$C(S)=D(S)/F(S)$$

称为S的**因子类群**。

设h的因子$(h)=0$，h有什么性质？我们先证明：

引理 2 设S是正规诺德整环，那么任意的主理想(a)的相伴素理想$\mathfrak{p}_i$都有相同的高度1。

证明 应用Krull主理想定理，(a)的孤立的相伴素理想的高度都是1。所以只要证明(a)没有嵌入素理想便足够了。

假设(a)有相伴的素理想$\mathfrak{p}\subsetneqq\mathfrak{q}$。对$\mathfrak{q}$作局部化后，$aS_{\mathfrak{q}}$有相

伴素理想 $\mathfrak{p}S_\mathfrak{q} \subsetneqq \mathfrak{q}S_\mathfrak{q}$。根据定理6.21的证明，存在 $b \in S_\mathfrak{q}$，使得 $\mathfrak{q}S_\mathfrak{q} = (aS_\mathfrak{q} : b)$，此处 $b \overline{\in} aS_\mathfrak{q}$（否则，$(aS_\mathfrak{q} : b) = S_\mathfrak{q}$）。于是

$$b(\mathfrak{q}S_\mathfrak{q}) \subset aS_\mathfrak{q}, \qquad (b/a)(\mathfrak{q}S_\mathfrak{q}) \subset S_\mathfrak{q}.$$

不难看出，$(b/a)(\mathfrak{q}S_\mathfrak{q})$ 是 $S_\mathfrak{q}$ 的一个理想。只有两种可能：

1）$(b/a)(\mathfrak{q}S_\mathfrak{q}) = S_\mathfrak{q}$；

2）$(b/a)(\mathfrak{q}S_\mathfrak{q}) \subset \mathfrak{q}S_\mathfrak{q}$。

在情形1）下，存在 $c \in \mathfrak{q}S_\mathfrak{q}$，使 $(b/a) \cdot c = 1$，即有

$$a = bc, \qquad (c) = (aS_\mathfrak{q} : b) = \mathfrak{q}S_\mathfrak{q},$$

故

$$\dim S_\mathfrak{q} \leqslant 1.$$

这与 $S_\mathfrak{q}$ 中存在素理想链 $0 \subsetneqq \mathfrak{p}S_\mathfrak{q} \subsetneqq \mathfrak{q}S_\mathfrak{q}$（即 $\dim S_\mathfrak{q} \geqslant 2$）不合。所以情形1）是不可能发生的。

在情形2）下，令 $d = b/a$，$\mathfrak{q}S_\mathfrak{q} = (c_1, \cdots, c_r)$。那么，我们得出联立方程式

$$dc_i = \sum_j a_{ij} c_j, \qquad a_{ij} \in S_\mathfrak{q} \ (i = 1, \cdots, r).$$

不难得出（参见定理7.21及定理6.6的证明），d 对 $S_\mathfrak{q}$ 是整数相关的，所以 $d \in S_\mathfrak{q}$。即 $b = ad \in aS_\mathfrak{q}$，与 b 的已知性质矛盾。▌

讨论 当理想 I 的相伴素理想都有相同的高度时，我们称 I 是**不杂的**。在几何的情形下，不杂的理想 I 定义的多样体的各个分支有相同的维数。

定理7.22 设 S 是整环，那么，我们有

1）$S = \bigcap S_\mathfrak{p}$，$\mathfrak{p}$ 取所有可能的素理想；

2）$S = \bigcap S_\mathfrak{m}$，$\mathfrak{m}$ 取所有可能的极大理想；

3）如果 S 是正规诺德环，则 $S = \bigcap S_\mathfrak{p}$，$\mathrm{ht}(\mathfrak{p}) = 1$。

证明 1）显然有 $S \subset S_\mathfrak{p}$，$S \subset \bigcap S_\mathfrak{q}$。任取 $a/b \overline{\in} S$，$a, b \in S$。这就是说 $a \overline{\in} (b)$。令 $\mathfrak{p}$ 是与 $\{a^n: n = 0, 1, 2, \cdots\}$ 交集为空集而且含有 b 的所有理想中的极大者，不难看出，$\mathfrak{p}$ 是一个素理想。在 $S_\mathfrak{p}$ 中，a 是可逆元，b 不是可逆元，因此 $a/b \overline{\in} S_\mathfrak{p}$。

2）任取素理想 $\mathfrak{p}$，设极大理想 $\mathfrak{m} \supset \mathfrak{p}$。显然有 $S_\mathfrak{m} \subset S_\mathfrak{p}$。

3）应用定理7.21，$S_\mathfrak{p}$都是一秩离散赋值环。令$v_\mathfrak{p}$是与$S_\mathfrak{p}$相对应的赋值。任取 $b/a\in \bigcap S_\mathfrak{p}(\mathrm{ht}(\mathfrak{p})=1)$，立得

$$v_\mathfrak{p}\left(\frac{b}{a}\right)\geqslant 0,\quad v_\mathfrak{p}(b)\geqslant v_\mathfrak{p}(a).$$

设(a)，(b)的简略准素分解如下：

$$(a)=\bigcap I_i,\quad \sqrt{I_i}=\mathfrak{p}_i,$$
$$(b)=\bigcap J_j,\quad \sqrt{J_j}=\mathfrak{q}_j.$$

应用引理，$\mathrm{ht}(\mathfrak{p}_i)=\mathrm{ht}(\mathfrak{q}_j)=1(\forall i,j)$。于是

$$v_{\mathfrak{p}_i}(b)\geqslant v_{\mathfrak{p}_i}(a),\quad v_{\mathfrak{q}_j}(b)\geqslant v_{\mathfrak{q}_j}(a).$$

不难得出，$\{\mathfrak{p}_i\}\subset\{\mathfrak{q}_j\}$，以及

$$(a)S_{\mathfrak{q}_j}\supset(b)S_{\mathfrak{q}_j}.$$

不妨设 $\mathfrak{p}_i=\mathfrak{q}_i$，如果 $\mathfrak{q}_j\overline{\in}\{\mathfrak{p}_i\}$，则令 $I_j=S$。经过这样的整理以后，由

$$(a)S_{\mathfrak{p}_i}=I_iS_{\mathfrak{p}_i},\quad (b)S_{\mathfrak{q}_j}=J_jS_{\mathfrak{q}_j},$$

即知

$$I_jS_{\mathfrak{q}_j}\supset J_jS_{\mathfrak{q}_j},\quad \forall j.$$

现在要说明

$$I_jS_{\mathfrak{q}_j}\cap S=I_j,\quad J_jS_{\mathfrak{q}_j}\cap S=J_j.$$

显然，$I_jS_{\mathfrak{q}_j}\cap S\supset I_j$。任取$c\in I_jS_{\mathfrak{q}_j}\cap S$，那么$c=r/s$，其中 $r\in I_j$，$s\overline{\in}\mathfrak{q}_j$，$c\in S$。如果$I_j=S$(即 $\mathfrak{q}_j\overline{\in}\{\mathfrak{p}_i\}$时)，则显然 $c\in I_j$。否则I_j是S的准素理想，$\sqrt{I_j}=\mathfrak{q}_j$。由 $r=cs$，根据准素理想的定义，即知$c\in I_j$。于是 $I_jS_{\mathfrak{q}_j}\cap S=I_j$.类似地可证

$$J_jS_{\mathfrak{q}_j}\cap S=J_j.$$

所以，我们得出

$$I_j=I_jS_{\mathfrak{q}_j}\cap S\supset J_jS_{\mathfrak{q}_j}\cap S=J_j.$$

于是有

$$(a)=\bigcap I_j\supset\bigcap J_j=(b),\quad b\in(a),$$

即有

$$b/a\in S.\ \blacksquare$$

讨论 在几何的情形下，$S=k[x_1,\cdots,x_n]$等于一个代数多样体V的**多项式函数环**。$S_\mathfrak{m}$是在$\mathfrak{m}$定义的一点上的不等于∞的有理函数环。定义7.22的2)的意义是：在V上有定义的多项式函

数，即是在各点都不等于∞的有理函数。

在代数的情形下，引用谱集Spec S，我们把S的比域K中的元素当作在Spec S上定义的函数，把S当作Spec S上的多项式函数。那么，定理7.22的2）也有与上面相同的意义。

系 设$S=k[x_1,\cdots,x_r]$是正规整环，K是它的比域，$f\in K$。那么，因子$(f)=0\Longleftrightarrow f$是$S$的可逆元。

证明 $v_\mathfrak{p}(f)=0\Longleftrightarrow v_\mathfrak{p}(f^{-1})=0\Longleftrightarrow f,f^{-1}\in S_\mathfrak{p}$。 ▌

一般说来，因子群$D(S)$是一个很大的自由交换群，提供不了什么有用的数据，而因子类群$C(S)$是可以表现一些有用的现象的。我们先证明下面的引理。

引理3 设S是诺德整环，那么，下面的三个性质是等同的：

1） S是唯一分解整环；

2） S的不可分解的元素f都生成素理想；

3） 高度为1的素理想都是主理想。

证明 在S是诺德环的条件下，我们已有分解的存在性，以下仅讨论分解的唯一性。

1）$\Longrightarrow$2）．设S是唯一分解的整环，f是不可分解的元素。设$gh\in(f)$，即存在$h'\in S$，使$gh=fh'$。于是，$f|g$或$f|h$，即$g\in(f)$或$h\in(f)$。因此(f)是一个素理想。

2）$\Longrightarrow$1）．设

$$(*)\qquad \prod f_i=\prod g_j,$$

f_i,g_j都是不可分解的。那么$\prod g_j\in(f_i)$，必有某个$g_j\in(f_i)$，即$f_i|g_j$。因g_j也是不可分解的，不难导出f_i与g_j相伴。我们从（$*$）式两侧消去f_i以后，应用归纳法，便可得出分解的唯一性。

2）$\Longrightarrow$3）。设$\mathrm{ht}(\mathfrak{p})=1$。取不可分解元$f\in\mathfrak{p}$，那么$(f)\subset\mathfrak{p}$，于是$(f)=\mathfrak{p}$。

3）$\Longrightarrow$2）．取包含(f)的极小素理想$\mathfrak{p}$。根据Krull主理

想定理，$\mathrm{ht}(\mathfrak{p})=1$。因此 $\mathfrak{p}=(y)\ni f$，立得 $f=gh$。所以 f,g 是相伴的，$(f)=\mathfrak{p}$。▎

下面的定理告诉我们因子类群的一个用途。

定理7.23 设 $S=k[x_1,\cdots,x_r]$ 是正规整环。则 S 是唯一分解的整环 $\Longleftrightarrow C(S)=0$。

证明 $\Longrightarrow$。设 W 对应于素理想 $\mathfrak{p}$，$\mathrm{ht}(\mathfrak{p})=1$。根据上面的引理，$\mathfrak{p}=(f)$。所以（参见例20后面引入的记号）

$$\text{主因子}(f)=\sum v_{w_i}(f)W_i=W。$$

立得 $D(S)=F(S)$，$C(S)=0$。

$\Longleftarrow$。任取一个高度为 1 的素理想 $\mathfrak{p}$，令 W 与它对应。那么，存在 f，使

$$\text{主因子}(f)=W,$$

即 $v_w(f)=1$，$\mathfrak{p}\ni f$，$v_{w_i}(f)=0$，$\forall W_i\neq W$。这就是说，对于任一高度为 1 的素理想 $\mathfrak{p}_i\neq\mathfrak{p}$，总有 $f\notin\mathfrak{p}_i$。利用定理7.22的3)，立得

$$(f)=fS=f\left(\bigcap_i S_{\mathfrak{p}_i}\cap S_{\mathfrak{p}}\right)=\left(\bigcap_i fS_{\mathfrak{p}_i}\right)\cap fS_{\mathfrak{p}}$$

$$=\left(\bigcap_i S_{\mathfrak{p}_i}\right)\cap\mathfrak{p}S_{\mathfrak{p}}=\mathfrak{p}\left(\bigcap_i S_{\mathfrak{p}_i}\cap S_{\mathfrak{p}}\right)=\mathfrak{p}S=\mathfrak{p}.$$

这就是说，高度为 1 的素理想都是主理想。应用引理 3，立得本定理。▎

例21 设 $S=\mathbf{C}[x,y]/(x^2-y(y-1))\supset\mathbf{C}[y]$，$K$ 是 S 的比域。

1) S 是正规的。我们只须证明 S 是 $\mathbf{C}[y]$ 在 K 中的整数闭包 $\overline{\mathbf{C}[y]}$ 便足够了。显然，x 对 $\mathbf{C}[y]$ 是整数相关的，所以 $S\supset\overline{\mathbf{C}[y]}$。在 K 中任取对 $\mathbf{C}[y]$ 整数相关的元素 $\alpha(y)x+\beta(y)$，此处 $\alpha(y)$，$\beta(y)\in\mathbf{C}(y)$。它的迹和范数

$$\mathrm{Tr}(a(y)x+\beta(y))=2\beta(y),$$

$$\mathrm{N}(a(y)x+\beta(y))=-a^2(y)(y(y-1))+\beta^2(y)$$

都应属于 $\boldsymbol{C}[y]$。于是

$$\beta(y)\in\boldsymbol{C}[y],$$

$$a^2(y)y(y-1)\in\boldsymbol{C}[y]\Longrightarrow a(y)\in\boldsymbol{C}[y].$$

所以 $S=\overline{\boldsymbol{C}[y]}$。

2) 设 v 是对 S 的第一类素因子，σ: $R_v\to\Delta_v=R_v/\mathfrak{m}_v=\boldsymbol{C}$ 是典型映射。设 $\sigma(x)=a$，$\sigma(y)=b$。不难看出，

$$\mathfrak{p}=\mathfrak{m}_v\cap S=(x-a,y-b)S,$$

即 v 对应到曲线

$$x^2-y(y-1)=0$$

上的一点(a,b)。反之，任取曲线上的一点(a,b)，考虑素理想

$$(x-a,y-b)=\mathfrak{p}.$$

因为 $\dim S=\dim\boldsymbol{C}[y]=1$，所以 $\mathrm{ht}(\mathfrak{p})\leqslant1$。于是显然，$\mathrm{ht}(\mathfrak{p})=1$。所以 $S_{\mathfrak{p}}$ 是对 S 的第一类素因子。综上所述，因子群 $D(S)$ 即是曲线上的点所生成的自由交换群

$$\left\{\sum n_iW_i:\ W_i\ \text{是曲线上的点}\right\}.$$

3) 任取曲线上一点(a,b)。考虑下面的多项式

$$f(x,y)=x+y-a-b\in S,$$

读者自行验证 S 的理想$(f)=(x-a,y-b)$。于是

$$\text{因子}(f)=(a,b).$$

因此，$C(S)=D(S)/F(S)=0$。所以 S 是唯一分解的整环。

例22 设 $S=\boldsymbol{C}[x,y]/(x^2-y(y-1)(y-2))\supset\boldsymbol{C}[y]$，$K$ 是 S 的比域。就像上面的例子一样，我们可以验证

1) S 是正规的；

2) $D(S)=\left\{\sum n_iW_i:\ W_i\ \text{是曲线}\ x^2-y(y-1)(y-2)=0\ \text{上的点}\right\}$；

3) $C(S)\neq 0$，这就是说，S不是唯一分解的整环。为证明这一点，应用引理 3，我们仅须证明素理想$(\bar{x},\bar{y})$不是主理想便可以了。

假设 $(\bar{x},\bar{y})=(g(\bar{x},\bar{y}))$。令 $f(x,y)=x^2-y(y-1)(y-2)$，立得

$$(x,y)=(g(x,y),f(x,y)).$$

不难看出（为什么？）

$$g(x,y)=\alpha(y)x+\beta(y)\neq y,\qquad (\alpha(y),\beta(y))=(1).$$

我们要说明$(g(x,y),f(x,y))\cap \mathbf{C}[y]=(h(y))$，此处

$$h(y)=\beta^2(y)-\alpha^2(y)y(y-1)(y-2).$$

从这里立刻可以导出 $\deg h(y)\neq 1$，$h(y)\overline{\in}\mathbf{C}$，所以 $y\overline{\in}(h(y))$，

$$(x,y)\cap \mathbf{C}[y]\neq(g(x,y),f(x,y))\cap \mathbf{C}[y],$$

$$(x,y)\neq(g(x,y),f(x,y)).$$

设 $r(y)$是$(g(x,y),f(x,y))\cap \mathbf{C}[y]$中的任一多项式。则存在 $a(x,y),b(x,y)\in \mathbf{C}[x,y]$，使

$$(1)\qquad r(y)=a(x,y)g(x,y)+b(x,y)f(x,y).$$

用欧几里得算法，有

$$a(x,y)=d(x,y)f(x,y)+a'(x,y),\quad \deg_x a'(x,y)\leqslant 1.$$

代入(1)式，得

$$r(y)=a'(x,y)g(x,y)+b'(x,y)f(x,y).$$

比较两侧 x 的次数，不难看出

$$\deg_x a'(x,y)=1,\qquad \deg_x b'(x,y)=0$$

令

$$a'(x,y)=\delta(y)x+\varepsilon(y),\qquad b'(x,y)=\pi(y).$$

于是得

$$(2)\quad r(y)=(\delta x+\varepsilon)(\alpha x+\beta)+\pi(x^2-y(y-1)(y-2)).$$

比较两侧 x 的系数，有

$$\delta\alpha=-\pi,\qquad \delta\beta+\varepsilon\alpha=0.$$

因为$(\alpha,\beta)=(1)$，所以 $\delta=\lambda\alpha$，$\varepsilon=-\lambda\beta$，$\pi=-\lambda\alpha^2$，其中 $\lambda\in$

$\boldsymbol{C}[y]$。代入(2)式，即得

$$r(y)=-\lambda h(y).$$

习　题

1. 令$R=\boldsymbol{C}[x,y]/(x^2-y^2-x^3)$。证明$R$是整环，试求$R$的比域$K$的一个第一类素因子。

2. 续上题。证明R不是整数封闭的。

3. 令$R=\boldsymbol{C}[x,y]/(y^2-x^2+1)$，证明$R$是整闭整环。

4. 续上题。试确定R的比域K的所有第一类素因子。

5. 续上题。判断R是否唯一分解整环。

6. 设题3中整环R的比域为K。又设x，y在典型映射下在R内的象为$\bar{x}$，$\bar{y}$，令$f=-3+\bar{x}^2\bar{y}\in K$。试计算$f$的主因子$(f)$。

7. 设$f(x,y)$是$\boldsymbol{C}[x,y]$内不可约多项式，由它生成的理想(f)对应的不可约代数多样体$\mathscr{V}(f)$上每一个点都是平滑的。令$R=\boldsymbol{C}[x,y]/(f(x,y))$，$R$的比域$K$的因子群中一元素

$$a=\sum n_i W_i,$$

其次数定义为$\deg a=\sum_i n_i$。如果所有$n_i\geqslant 0$，则a称为正因子。给定因子a，令$L(a)$表示K中满足如下条件的元素u所成的集合：$(u)+a$为正因子。证明$L(a)$是域$\boldsymbol{C}$上的一个线性空间。

8. 续上题。设$u\in K\backslash\boldsymbol{C}$。令

$$(u)_0=\sum_{v_w(u)>0} v_w(u)W,\qquad (u)_\infty=\sum_{v_w(u)<0} v_w(u)W.$$

证明：$\deg(u)_0=-\deg(u)_\infty=[K:\boldsymbol{C}(u)]$，从而$\deg u=0$。

第八章 Dedekind 整环

§1 定　义

本章的题材主要源自“代数数论”及“仿射代数曲线论”。仿射代数曲线加上无穷远点集即是射影代数曲线，也即相当于黎曼曲面。因此，本章的结果可以应用到数论、几何学及复变函数论。

设K是Q的有限代数扩域。我们要研究K的代数整数环S。显然，S应该包含1，S应该以K为比域，S应该是整数封闭的（即S是正规环）。在上面的三个自然条件下，S的自然选择应该是 $\boldsymbol{Z}$ 在K中的整数闭包。此时，S是一维正规诺德整环(参见定理6.7与6.23，以及下面的定理8.3)。

设k是一个常数域，C是一个一维仿射正则代数曲线，S是C的多项式函数环，$S=k[x_1,\cdots,x_n]$。这时，S是一个正则环，即对任意的极大理想 $\mathfrak{p}$ 而言，$S_{\mathfrak{p}}$是正则局部环。由于S是一维的，所以 $\mathrm{ht}(\mathfrak{p})=1$。根据定理7.21，$S_{\mathfrak{p}}$都是赋值环，因此都是整数封闭的。根据定理7.22，我们知道

$$S=\bigcap S_{\mathfrak{p}},$$

因此S也是整数封闭的(事实上，只要S是正则诺德环，S一定是正规的)。所以S是一个一维正规诺德整环。

综上所述，我们给出如下的定义：

定义8.1 设D是一个整环。若D适合下面的条件：

1) D是诺德环；

2) D是正规的；

3) $\dim D\leqslant 1$。

则称之为 Dedekind **整环**。

讨论 1) 如果 $\dim D=0$，则 D 是域。如果 $\dim D=1$，则 D 是一维正规诺德整环。

2) Artin 环的定义是什么？ ▌

在本节里，我们将证明 Dedekind 整环的一些等价的定义。先引入"分理想"的概念。设 S 是一个整环，K 是它的比域，J 是 K 的一个子集，而且是 S 模。如果 J 的所有元素有一个公分母 d，即 $J\subset(1/d)S$，那么，J 就称为一个**分理想**。显然，S 的理想 I 有公分母 1，$I\subset S$，所以 I 是一个分理想。S 的理想 I 也称为**整理想**。形如 $(a/b)S$ 的分理想称为**主分理想**。

固定了 S 以后，令 $\mathscr{F}$ 是所有分理想的集合。那么，在 $\mathscr{F}$ 中有自然的"+"，"·"，"∩"等运算。我们可以定义运算":"（即"比"）：

$$J_1:J_2=\{a:\ a\in K,\ aJ_2\subset J_1\}.$$

不难看出，$J_1:J_2$ 是一个 S 模。设 $J_2\neq(0)$，令 d_1 是 J_1 的公分母，任取 $b\in J_2$，$b\neq0$，显然有 $d_1b(J_1:J_2)\subset S$，所以当 $J_2\neq(0)$ 时，$J_1:J_2$ 也是一个分理想。

对"·"而言，S 显然是 $\mathscr{F}$ 的幺元：$SJ=J$。我们定义非零的分理想 J 的**拟逆元**：

$$J^{-1}=\{a:\ aJ\subset S\}=S:J.$$

请注意，JJ^{-1} 不一定等于 S，当 $JJ^{-1}=S$ 时，我们称 J 是**可逆的**。当 J 为非零的主分理想 $(a/b)S$ 时，

$$J^{-1}=(b/a)S,\qquad JJ^{-1}=S,$$

故 J 是可逆的。

我们先证明一些引理。

引理 1 设 $J\in\mathscr{F}$。如果 J' 是 J 的一个乘法逆元，则

$$J'=J^{-1}.$$

证明 设 J' 是 J 的乘法逆元，则 $JJ'\subset S$。那么 $J'\subset S:J=J^{-1}$。我们又有 $S:J=J'J(S:J)\subset J'S=J'$，所以 $J'=J^{-1}$。 ▌

引理 2 如果每一非零整理想 I 都是可逆的，那么$\mathscr{F}\backslash\{(0)\}$是一个乘法群。

证明 取 $J\in\mathscr{F}\backslash\{(0)\}$。则存在 d，使 $J=(1/d)I$，此处 I 是一个整理想。显然，

$$J^{-1}=dI^{-1}\quad (JJ^{-1}=(1/d)IdI^{-1}=S)。\ \blacksquare$$

引理 3 每一个可逆的分理想 J 必定是一个有限 S 模。

证明 已知 $JJ^{-1}=S$。那么，存在有限集$\{a_i\}\subset J$，$\{a'_i\}\subset J^{-1}$，使

$$\sum a_i a'_i=1。$$

任取 $a\in J$，显然 $aa'_i\in S$。于是

$$a=a\sum a_i a'_i=\sum(aa'_i)a_i,$$

可见$\{a_i\}$是 J 的生成元集。$\blacksquare$

引理 4 设 $I_1,\cdots,I_n$ 是整理想，$\prod\limits_{i=1}^{n} I_i$ 是可逆的，那么每个 $I_j(j=1,\cdots,n)$都是可逆的。

证明 令 J 是$\prod\limits_{i=1}^{n}I_i$ 的乘法逆元，那么$I_j\left(J\prod\limits_{i\neq j}I_i\right)=S$。$\blacksquare$

引理 5 设 $\mathfrak{p}_1,\cdots,\mathfrak{p}_n$ 是可逆的素整理想，$\mathfrak{q}_1,\cdots,\mathfrak{q}_l$ 是素整理想，

$$(*)\qquad \prod\mathfrak{p}_i=\prod\mathfrak{q}_j。$$

那么，$n=l$，且经过整理以后，有 $\mathfrak{p}_1=\mathfrak{q}_1,\cdots,\mathfrak{p}_n=\mathfrak{q}_n$。

证明 设 $\mathfrak{p}_1$是$\{\mathfrak{p}_1,\cdots,\mathfrak{p}_n\}$中的极小者。由于

$$\mathfrak{p}_1\supset\prod\mathfrak{p}_i=\prod\mathfrak{q}_j,$$

所以必有某个 $\mathfrak{q}_j\subset\mathfrak{p}_1$。同理，必有某个

$$\mathfrak{p}_s\subset\mathfrak{q}_j。$$

由 $\mathfrak{p}_1 \supset \mathfrak{q}_j \supset \mathfrak{p}_s$，立得 $\mathfrak{p}_1 = \mathfrak{q}_j = \mathfrak{p}_s$。在(*)式两侧乘以 $\mathfrak{p}_1^{-1}$，应用归纳法立得本引理。

引理 6 设 S 是正规诺德整环，$a \in S$。设 $\mathfrak{p}$ 是主理想 Sa 的相伴素理想。如果 $\mathfrak{p}$ 是一个极大理想，那么，$\mathfrak{p}$ 是可逆的。

证明 假设 $\mathfrak{p}$ 不是可逆的。那么 $\mathfrak{p} \subset \mathfrak{p}(S:\mathfrak{p}) \subsetneqq S$。因为 $\mathfrak{p}$ 是极大理想，而 $\mathfrak{p}(S:\mathfrak{p})$ 是 S 的理想，所以 $\mathfrak{p} = \mathfrak{p}(S:\mathfrak{p})$。于是，任取 $r \in (S:\mathfrak{p})$，则有 $r\mathfrak{p} \subset \mathfrak{p}$。因为 S 是诺德环，所以可令

$$\mathfrak{p} = (b_1, \cdots, b_n).$$

不难看出，我们得出一组联立方程式

$$rb_i = \sum_j c_{ij} b_j, \quad c_{ij} \in S \ (i = 1, \cdots, n).$$

所以，r 适合 $[c_{ij}]$ 的特征多项式

$$\det(rI - [c_{ij}]) = 0.$$

因此 r 对 S 是整数相关的。已知 S 是正规的，所以 $r \in S$。于是，

$$(S:\mathfrak{p}) \subset S.$$

又显然 $(S:\mathfrak{p}) \supset S$，故有 $(S:\mathfrak{p}) = S$，以及 $(Sa:\mathfrak{p}) = Sa$。以下我们要证明，在诺德环里，$\mathfrak{p}$ 为极大理想，那么 $(Sa:\mathfrak{p}) = Sa$ 与 $\mathfrak{p}$ 是 Sa 的相伴素理想，二者不能相容。

令 $Sa = \bigcap \mathfrak{q}_i$ 是 Sa 的简略准素分解，$\sqrt{\mathfrak{q}_1} = \mathfrak{p}$。设 $\mathfrak{q}_1 \supset \mathfrak{p}^l$。我们有

$$Sa = (Sa:\mathfrak{p}) = ((Sa:\mathfrak{p}):\mathfrak{p}) = (Sa:\mathfrak{p}^2) = \cdots = (Sa:\mathfrak{p}^l)$$
$$= (\bigcap \mathfrak{q}_i:\mathfrak{p}^l) = \bigcap (\mathfrak{q}_i:\mathfrak{p}^l) = \bigcap ((\mathfrak{q}_i:\mathfrak{p}^l) \cap S).$$

显然 $(\mathfrak{q}_1:\mathfrak{p}^l) \cap S = S$。我们要说明 $(\mathfrak{q}_i:\mathfrak{p}^l) \cap S = \mathfrak{q}_i (\forall i \neq 1)$。这只要说明 $(\mathfrak{q}_i:\mathfrak{p}) \cap S \subset \mathfrak{q}_i$。任取 $b \in (\mathfrak{q}_i:\mathfrak{p}) \cap S$，则 $b\mathfrak{p} \subset \mathfrak{q}_i$。假若 $b \bar{\in} \mathfrak{q}_i$，由于 $\mathfrak{p}$ 是有限生成的理想，必有充分大的整数 m，使

$$\mathfrak{p}^m \subset \mathfrak{q}_i \subset \sqrt{\mathfrak{q}_i} = \mathfrak{p}_i,$$

于是 $\mathfrak{p} \subset \mathfrak{p}_i$。而 $\mathfrak{p}$ 是极大理想，所以 $\mathfrak{p} = \mathfrak{p}_i$。这与简略准素分解的定义相矛盾。因此必有 $b \in \mathfrak{q}_i$，则

$$(\mathfrak{q}_i:\mathfrak{p})\cap S\subset\mathfrak{q}_i.$$

于是，我们得出了 Sa 的另一个简略准素分解

$$Sa=\bigcap_{i\neq 1}\mathfrak{q}_i.$$

这是不可能的。▌

引理 7 设 S 是一个诺德整环。如果 S 的每个极大理想都是可逆的，那么，每一个非零的理想 I 都是 S 的极大理想的乘积。

证明 设有一个非零的整理想不是极大理想的乘积，根据诺德环的条件，必有一个整理想 I 是适合此种条件的整理想中的极大者。自然，I 不是极大理想。设 $I\subsetneqq\mathfrak{m}$，$\mathfrak{m}$ 是极大理想。考虑 $\mathfrak{m}^{-1}I$。显然有 $I\subset\mathfrak{m}^{-1}I\subset S$。

假若 $I=\mathfrak{m}^{-1}I$，立得 $\mathfrak{m}I=I$。应用中山引理的证明，易于得出，存在 $a\in\mathfrak{m}$，使 $(1-a)I=(0)$。那么，$I=(0)$，与 I 是非零整理想矛盾。所以 $I\subsetneqq\mathfrak{m}^{-1}I$。根据 I 的选取，

$$\mathfrak{m}^{-1}I=\prod\mathfrak{m}_i,$$

这里 $\mathfrak{m}_i$ 是 S 的极大理想，即 $I=\mathfrak{m}\prod\mathfrak{m}_i$。这与 I 的选法矛盾。▌

请注意下面的定理的条件3)。一般说来，在代数整数环里，沒有整数的唯一分解定理。Kummer 发现了“理想的唯一分解定理”，弥补了部分缺憾。

定理8.1 设 D 是一整环。那么，下面的三个条件是等同的：

1) D 是 Dedekind 整环；

2) 如果 D 不是域，则 $\mathscr{F}\setminus(0)$ 是一个乘法群；

3) 每一个理想 I 可以唯一地写成素理想的乘积 $I=\prod\mathfrak{p}_i$。

证明 1) $\Longrightarrow$ 3)。我们只须讨论 D 不是域，$I\neq(0)$ 的情形。于是，$\dim D=1$。任取一个素理想 $\mathfrak{p}\neq(0)$，那么，$\mathfrak{p}$ 是一极大理想。任取 $0\neq a\in\mathfrak{p}$。显然，$\mathfrak{p}$ 包含 Da 的一个相伴素理想；因此 $\mathfrak{p}$

是 Da 的一个相伴素理想。我们应用引理 6，得出 $\mathfrak{p}$ 是可逆的。再应用引理 7，得出每一个理想 I 都是极大理想的乘积；又根据引理 5，得出乘积的唯一性。

3)$\Longrightarrow$2)。仅须证明每一个非零的分理想 J 都是可逆的。设 $J\subset(1/d)D$。不难看出，$dJ=I$ 是 D 的理想。令

$$I=\prod \mathfrak{p}_i,\quad (d)=\prod \mathfrak{q}_j.$$

我们先证明每一个非零素理想 $\mathfrak{p}$ 都是可逆的。任取 $0\neq a\in\mathfrak{p}$，设

$$Sa=\prod \mathfrak{p}'_i\subset\mathfrak{p}.$$

由于主理想都是可逆的，应用引理 4，那么，每个 $\mathfrak{p}'_i$ 都是可逆的。此时，$\mathfrak{p}$ 必包含某个 $\mathfrak{p}'_i$，所以我们只要证明：在 3)的条件下，每一个可逆的素理想都是极大理想（如此，则 $\mathfrak{p}\supset\mathfrak{p}'_i\Longrightarrow\mathfrak{p}=\mathfrak{p}'_i\Longrightarrow\mathfrak{p}$ 可逆）。

任取 $b\in D\backslash\mathfrak{p}'_1$，$\mathfrak{p}'_1$ 是一个可逆的素理想。考虑

$$\mathfrak{p}'_1+Db,\quad \mathfrak{p}'_1+Db^2.$$

根据条件3)，我们有下式

$$\mathfrak{p}'_1+Db=\prod \mathfrak{q}'_k,\quad \mathfrak{p}'_1+Db^2=\prod \mathfrak{q}''_l,$$

此处 $\mathfrak{q}'_k,\mathfrak{q}''_l$ 都是素理想。自然，$\mathfrak{q}'_k\supset\mathfrak{p}'_1,\mathfrak{q}''_l\supset\mathfrak{p}'_1$。作典型映射 σ: $D\to\bar{D}/\mathfrak{p}'_1$，立得

$$\bar{D}\bar{b}=\sigma(\mathfrak{p}'_1+Db)=\prod \mathfrak{q}'_k/\mathfrak{p}'_1,$$

$$\bar{D}\bar{b}^2=\sigma(\mathfrak{p}'_1+Db^2)=\prod \mathfrak{q}''_l/\mathfrak{p}'_1.$$

利用引理 4，主理想 $\bar{D}\bar{b}$ 与 $\bar{D}\bar{b}^2$ 都是可逆的，于是 $\mathfrak{q}'_k/\mathfrak{p}'_1,\mathfrak{q}''_l/\mathfrak{p}'_1$ 都是可逆的素理想。但 $(\bar{D}\bar{b})^2=\bar{D}\bar{b}^2$，应用引理 5，即知 $\{\mathfrak{q}''_l/\mathfrak{p}'_1\}$ 是 $\{\mathfrak{q}'_k/\mathfrak{p}'_1\}$ 的两倍重复，即有

$$\mathfrak{p}'_1\subset\mathfrak{p}'_1+Db^2=\prod \mathfrak{q}''_l=\left(\prod \mathfrak{q}'_k\right)^2=(\mathfrak{p}'_1+Db)^2\subset(\mathfrak{p}'_2)^2+Db.$$

任取 $c\in\mathfrak{p}'_1$，由上式即知，存在 $d_1,d_2\in\mathfrak{p}'_1$，$s\in D$，使

$$c = d_1 d_2 + sb.$$

因为$b \bar{\in} \mathfrak{p}_1'$，所以$s \in \mathfrak{p}_1'$。于是$\mathfrak{p}_1' \subset (\mathfrak{p}_1')^2 + \mathfrak{p}_1' b \subset \mathfrak{p}_1'$，即有

$$\mathfrak{p}_1' = (\mathfrak{p}_1')^2 + \mathfrak{p}_1' b = \mathfrak{p}_1'(\mathfrak{p}_1' + Db).$$

由于$\mathfrak{p}_1'$是可逆的，以$(\mathfrak{p}_1')^{-1}$乘上式，得$D = \mathfrak{p}_1' + Db$。这就是说$\mathfrak{p}_1'$是极大理想。

上面已证明，每一个素理想$\mathfrak{p}_i, \mathfrak{q}_j$都是可逆的。回到起始处，

$$J = d^{-1} I = I(Dd)^{-1} = \prod \mathfrak{p}_i \left(\prod \mathfrak{q}_j \right)^{-1} = \prod \mathfrak{p}_i \prod \mathfrak{q}_j^{-1}$$

是可逆的。

2)$\Longrightarrow$3)。应用引理3，即知D是一诺德环。应用引理7，即知每一个非零的理想都可以分解成素理想的乘积。再应用引理5，得出分解的唯一性。

2)与3)$\Longrightarrow$1)。如果D是域，则D是Dedekind整环。我们仅须考虑D不是域的情形。

应用引理3，立得D是诺德环。先证D是一维的。应用引理7，我们可把任意的非零素理想$\mathfrak{p}$写成$\prod \mathfrak{m}_i$，$\mathfrak{m}_i$是极大理想。立得$\mathfrak{p}$包含一个极大理想，因此必然等于这个极大理想。所以D是一维的。

现在要证明D是正规的。应用定理7.22，我们仅须证明$D_{\mathfrak{p}}$是正规的，此处$\mathfrak{p}$是任意的非零素理想。只要证明$D_{\mathfrak{p}}$是一个赋值环就足够了。任给$a \in D$，令

$$(a) = \mathfrak{p}^n \prod \mathfrak{p}_i^{n_i}, \quad \mathfrak{p}_i \neq \mathfrak{p}.$$

定义$v(a) = n$。又若$v(b) = l$，那么

$$(a/b) = \mathfrak{p}^{n-l} \prod \mathfrak{p}_i^{*_i},$$

定义$v(a/b) = n - l = v(a) - v(b)$。显然$v$是一个一秩离散赋值。

现在我们要说明，v 的赋值环 $R_v = D_\mathfrak{p}$。不难看出，

$$v(b) = 0 \Longleftrightarrow b \overline{\in} \mathfrak{p},$$

此处 $b \in D$。因此 $R_v \supset D_\mathfrak{p}$。又设

$$\frac{a}{b} \in R_v,\ a, b \in D,\ (a) = \mathfrak{p}^n \prod \mathfrak{p}_i^{n_i},\ (b) = \mathfrak{p}^l \prod \mathfrak{p}_i^{l_i}.$$

则 $n \geqslant l$。那么

$$(a/b) D_\mathfrak{p} = \mathfrak{p}^{n-l} D_\mathfrak{p},$$

即存在 $c, d \in D$，使

$$\frac{a}{b} = \frac{c}{d},\quad c \in \mathfrak{p}^{n-l},\ d \in D \backslash \mathfrak{p},$$

也即 $a/b \in D_\mathfrak{p}$。所以 $R_v = D_\mathfrak{p}$。因此 D 是正规的。 ▌

定理8.2 设 D 是诺德整环。那么，D 是 Dedekind 整环 $\Longleftrightarrow$ 任取极大理想 $\mathfrak{p}$，$D_\mathfrak{p}$ 是赋值环。

证明 如果 D 是域，则无可证之处。设 D 不是域。

$\Longrightarrow$。$\mathfrak{p}$ 的高度是 1，应用定理7.21，立得。

$\Longleftarrow$。$D_\mathfrak{p}$ 是诺德环。应用定理7.3，立得 $\dim D_\mathfrak{p} = 1 (\forall\, \mathfrak{p})$。所以 $\dim D = 1$（定理6.26）。又根据定理7.22，立得 D 是正规的。 ▌

例 1 用第七章的例22。令

$$D = \mathbf{C}[x, y]/(x^2 - y(y-1)(y-2)).$$

不难验证，D 是一维正规诺德环，即 Dedekind 整环。在例22中，我们已经知道了 D 不是一个唯一分解的整环。但是 D 的每一个理想，都可以分解成素理想的唯一乘积。例如，考虑理想 $(\bar{y})$。现在我们要说明

$$(\bar{y}) = (\bar{x}, \bar{y})^2.$$

显然 $$\bar{x}^2 = \bar{y}(\bar{y}-1)(\bar{y}-2) \in (\bar{y}),$$

所以 $(\bar{y}) \supset (\bar{x}^2, \bar{x}\bar{y}, \bar{y}^2) = (\bar{x}, \bar{y})^2$。又有

$$\bar{y} = \frac{1}{2}(\bar{x}^2 - \bar{y}^3 + 3\bar{y}^2) \in (\bar{x}, \bar{y})^2,$$

立得$(\bar{y})=(\bar{x},\bar{y})^2$。从几何学的观点来看，这无非是说，$y=0$定义的曲线与$x^2-y(y-1)(y-2)=0$定义的曲线，在$(0,0)$点有一个重数为2的交点而已。

例2 令$S=\boldsymbol{Z}[\sqrt{-3}]$。此时$S$不是正规的，因为

$$\omega=(-1+\sqrt{-3})/2$$

在S的比域$\boldsymbol{Q}[\sqrt{-3}]$中，而且适合

$$\omega^2+\omega+1=0, \tag{1}$$

但是不在S中。令$D=\boldsymbol{Z}[\omega]$。不难看出，D是一个诺德环。现在要说明D是正规的。

任取$a+b\omega\in\boldsymbol{Q}[\omega]=\boldsymbol{Q}[\sqrt{-3}]$，$a,b\in\boldsymbol{Q}$。众所周知，$\omega^2$也适合(1)式，与$\omega$共轭。因此$a+b\omega^2$与$a+b\omega$共轭。由此可以算出

$$\mathrm{Tr}(a+b\omega)=(a+b\omega)+(a+b\omega^2)=2a-b,$$

$$\mathrm{N}(a+b\omega)=(a+b\omega)(a+b\omega^2)=a^2+b^2-ab.$$

设$a+b\omega$是对$\boldsymbol{Z}$整数相关的，那么，$a+b\omega^2$也对$\boldsymbol{Z}$整数相关，所以$2a-b\in\boldsymbol{Z}$，$a^2+b^2-ab\in\boldsymbol{Z}$。即有

$$2a-b=n, \quad n\in\boldsymbol{Z}, \tag{2}$$

$$a^2+b^2-ab=l, \quad l\in\boldsymbol{Z}. \tag{3}$$

解出(2)式中的b，代入(3)式，整理后，得

$$(3a)^2-3n(3a)+3(n^2-l)=0. \tag{4}$$

因$\boldsymbol{Z}$是整数封闭的(正规的)，所以$3a\in\boldsymbol{Z}$。由(4)式亦知$3\mid 3a$，所以$a\in\boldsymbol{Z}$。立得$b\in\boldsymbol{Z}$。这样，我们证明了D是$\boldsymbol{Z}$在$\boldsymbol{Q}[\omega]$中的整数闭包，因此是正规的。所以D是一个Dedekind整环，也就是$\boldsymbol{Q}[\sqrt{-3}]$中的代数整数环。 ▎

定理8.2建立了Dedekind整环与赋值论的联系。我们要进一步地发展两者的关系。

设D为Dedekind整环。令F为D的比域K的所有在D上为有限的非平凡的赋值v的集合。令R_v是v的赋值环，$\mathfrak{m}_v$是R_v的极大理想。令$\mathfrak{p}=\mathfrak{m}_v\cap D$。不难看出，$R_v=D_{\mathfrak{p}}$(定理7.21)。

因此 v 是一秩离散赋值。即

(K$_1$) F 中的赋值 v 都是一秩离散赋值。

又根据定理7.22，$D=\bigcap D_{\mathfrak{p}}=\bigcap R_v$，即

(K$_2$) D 是所有 R_v 的交集($v\in F$)。

任取 $0\neq a\in D$，$(a)=\prod_{i=1}^{r}\mathfrak{p}_i^{n_i}$。那么，当 $\mathfrak{p}\neq\mathfrak{p}_i(\forall i)$时，$v_{\mathfrak{p}}(a)=0$。因此有

(K$_3$) 任取 $0\neq a\in D$，除了有限多个 $v_i\in F$ 外，$v(a)=0$。

我们还有

(K$_4$) 任给 $v\in F$，恒有 $\mathfrak{p}\subset D$，使 $R_v=D_{\mathfrak{p}}$。

一般地，我们有下面的定义：

定义8.2 任何一个整环，适合上面的条件(K$_1$)，(K$_2$)，(K$_3$)，(K$_4$)，则称为一个 Krull **整环**。F 中的赋值 v，称为D**的主要赋值**。

讨论 1) 上面的讨论说明了，任意的 Dedekind 整环都是 Krull 整环。

2) 可以证明，$F=\{D_{\mathfrak{p}}:\ \mathrm{ht}(\mathfrak{p})=1\}$。

3) 可以证明，Krull 整环D是 Dedekind 整环$\Longleftrightarrow\dim D\leqslant 1$。

4) 任意正规诺德整环都是 Krull 整环。▍

以下，我们仿照第七章§6，构造 Dedekind 整环的因子类群。我们将仅应用条件(K$_1$)，(K$_2$)，(K$_3$)，(K$_4$)。所以，下面的讨论可以自然地推广到 Krull 整环上。

我们令 Dedekind 整环 S 的因子群

$$D(S)=\left\{\sum_{\text{有限}}n_iv_i:\ n_i\in\boldsymbol{Z},\ v_i\in F\right\},$$

其中F如前所述。任取 $a\in S$，令 a 的因子

$$(a)=\sum_i v_i(a)v_i.$$

应用(K_3)，上式右端是有限和，因此$(a)\in D(S)$。令

$$F(S)=\left\{\sum_{\text{有限}} n_j(a_j):\ a_j\in S\right\},$$

即为由因子(a) $(a\in S)$生成的子群。定义S的**因子类群**为

$$C(S)=D(S)/F(S).$$

因子类群又称为**理想类群**。

当 Dedekind 整环 $S=k[x_1,\cdots,x_n]$时(此处k是域)，这里定义的因子类群与第七章§6定义的因子类群是完全一样的，因为一个赋值v，只要在S上是有限的，必然是一个k赋值。

仿照定理7.22的系，我们也可以证明：因子$(a)=0\Longleftrightarrow a$是$S$的可逆元。在这个证明中，我们须应用$(\mathrm{K}_2)$。

仿照定理7.23，我们可以证明：S是唯一分解的整环$\Longleftrightarrow$ $C(S)=0$。

有兴趣的读者，请参考华罗庚著《数论导引》第十六章“代数数论介绍”中有关“单位数”(即上面提到的可逆元)、“理想类数”的讨论。

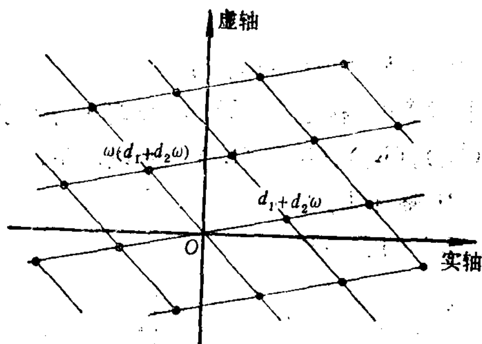


图 8.1

例3 我们在第一章§5中，已经证明了$\boldsymbol{Z}[\mathrm{i}]$是一个欧几里得整环(即存在欧几里得算法的整环)，因此是一个唯一分解的整环。所以

$$C(\boldsymbol{Z}[\mathrm{i}])=0.$$

现在我们返回去考虑例2，证明$C(\boldsymbol{Z}[\omega])=0$。证法与第一章§5类似。我们先在复平面上，对任

取的 $d_1+d_2\omega \neq 0$，作图8.1所示的网格。不难看出，任给一个 $a=a_1+a_2\omega$，a 必然在某一网格之中。网格是边长为$\sqrt{N(d_1+d_2\omega)}$的正菱形，于是必有一网格点$(b_1+b_2\omega)(d_1+d_2\omega)$与 a 的距离小于边长，即

$$N(a-(b_1+b_2\omega)(d_1+d_2\omega))<N(d_1+d_2\omega).$$

令 $r=a-(b_1+b_2\omega)(d_1+d_2\omega)$，$\beta=b_1+b_2\omega$，即得

$$a=\beta(d_1+d_2\omega)+r, \quad N(r)<N(d_1+d_2\omega).$$

所以，立得 $\boldsymbol{Z}[\omega]$是一个欧几里得整环。于是它是一个唯一分解的整环。所以 $C(\boldsymbol{Z}[\omega])=0$。

现在来计算 $\boldsymbol{Z}[\omega]$的可逆元。不难看出，$d_1+d_2\omega$ 是可逆元 $\Longleftrightarrow N(d_1+d_2\omega)=(d_1+d_2\omega)(d_1+d_2\omega^2)=1$。经进一步计算得

$$(d_1+d_2\omega)(d_1+d_2\omega^2)=(d_1^2+d_2^2)-d_1d_2=1.$$

在 $\boldsymbol{Z}[\omega]$中，满足上式的 $d_1+d_2\omega$ 只有$\{\pm1,\pm\omega,\pm(1+\omega)\}$，即是$\{\pm1,\pm\omega,\pm\omega^2\}$。

例 4 我们用例 3 的结果来解决费马问题的一个部分：下列方程式

$$x^3+y^3=z^3 \tag{1}$$

的整数解 x,y,z，必然是 x,y,z 三者之一为零。这就是说，x,y,z 必定是“平凡解”。

我们进一步研究 $\boldsymbol{Z}[\omega]$的算术结构。令 $\lambda=1-\omega$。那么，

$$N(\lambda)=(1-\omega)(1-\omega^2)=1-\omega-\omega^2+\omega^3=3.$$

3 是素整数，不难由此推知 λ 是不可分解的。现在，我们计算 $\boldsymbol{Z}[\omega]/(\lambda)$。显然

$$(\lambda)\cap\boldsymbol{Z}=(3),$$

$$\begin{aligned}\boldsymbol{Z}[\omega]/(\lambda)&\approx\boldsymbol{Z}[x]/(x^2+x+1,1-x)\\&\approx(\boldsymbol{Z}/(3))[x]/(x^2+x+1,1-x)\\&\approx(\boldsymbol{Z}/(3))[x]/(1-x)\approx\boldsymbol{Z}/(3).\end{aligned}$$

所以，任取 $a\in\boldsymbol{Z}[\omega]$，$a\equiv0$或 1 或 $-1 \pmod{\lambda}$。

我们考虑(1)式的非平凡的解组 x,y,z 的两种情形：$\lambda\nmid xyz$，

或 $\lambda \mid xyz$。

1) $\lambda \nmid xyz$。于是 $x,y,z\equiv\pm1 \pmod{\lambda}$。代入(1)式得

$$\pm1\pm1\equiv\pm1 \pmod{\lambda^3}.$$

但是 $3=-\omega^2\lambda^2$，所以 $\lambda^3\nmid 3$。因此不可能有上式。

2) $\lambda \mid xyz$。如果有这种不平凡的解组，那么，我们可以选取其中一组，使 xyz 有最少数目的不可分解的因子。不妨假设 $\lambda \mid z$。那么

$$\lambda|x \Longleftrightarrow \lambda|y \Longrightarrow \frac{x}{\lambda},\frac{y}{\lambda},\frac{z}{\lambda}\text{是因子数更少的解组。}$$

所以 $\lambda\nmid x$，$\lambda\nmid y$。设 $z=\lambda^s v$，$\lambda\nmid v$。考虑下面的比较广义的命题：设 μ 是 $\boldsymbol{Z}[\omega]$ 的可逆元，那么，下面的方程式

(2) $\qquad x^3+y^3+\mu\lambda^{3s}v^3=0,\qquad s\geqslant1,\ xyv\neq0,\ \lambda\nmid xyv$

在 $\boldsymbol{Z}[\omega]$ 中无解。

现在我们来证明这个命题。假设存在满足(2)的解组 x,y,v。对于 $s=1,2,\cdots$，(2)式给出一系列方程。考虑所有这些方程的所有可能的解，从其中选择一组 x,y,v，使 xyv 的因子数目为最少。读者容易证明，x,y,v 不可能都是 $\boldsymbol{Z}[\omega]$ 中的可逆元(因为这些可逆元的立方皆为 ±1)。如果 x,y 有不可分解的公因元 a，那么，$a\mid v$，这样，$x/a,y/a,v/a$ 又是一组解，而且因子数目更少。所以，在我们的选取下，必有

$$(x,y)=(y,v)=(x,v)=(1).$$

因为 $x^3+y^3\equiv x^3+y^3+\mu\lambda^{3s}v^3\equiv0 \pmod{\lambda}$，所以，

$$x\equiv\pm1 \pmod{\lambda},\qquad y\equiv\mp1 \pmod{\lambda}\quad\text{（为什么？）。}$$

不妨令 $x=1+\lambda a$，$y=-1+\lambda b$，此处 $a,b\in\boldsymbol{Z}[\omega]$。代入 x^3+y^3 后得(请注意 $3=-\omega^2\lambda^2$，$\omega\equiv1 \pmod{\lambda}$)：

$$\begin{aligned}x^3+y^3&=3\lambda(a+b)+3\lambda^2(a^2-b^2)+\lambda^3(a^3+b^3)\\&\equiv\lambda^3(-\omega^2(a+b)+(a^3+b^3))\\&\equiv\lambda^3(-(a+b)+(a^3+b^3)) \pmod{\lambda^4}.\end{aligned}$$

又不难看出，$a^3-a\equiv 0 \pmod{\lambda}$，$b^3-b\equiv 0 \pmod{\lambda}$，因此

$$x^3+y^3\equiv 0 \pmod{\lambda^4}.$$

结合(2)式，即知 $s\geqslant 2$。

(2)式又可以改写如下

(3) $$(x+y)(x+\omega y)(x+\omega^2 y)=-\mu\lambda^{3s}v^3.$$

在 $x\equiv 1 \pmod{\lambda}$，$y\equiv -1 \pmod{\lambda}$ 的假设下，不难看出，

$$\lambda \mid x+y,\quad \lambda \mid x+\omega y,\quad \lambda \mid x+\omega^2 y.$$

令

$$x'=\frac{x+\omega y}{\lambda},\quad y'=\frac{\omega(x+\omega^2 y)}{\lambda},\quad z'=\frac{\omega^2(x+y)}{\lambda},$$

则有 $x', y', z' \in \mathbf{Z}[\omega]$。因为

$$(1-\omega^2)x=\lambda x'-\lambda\omega y',$$

所以 x', y' 的公因子 β 必然是 x 的因子。同法可证 β 必然是 y 的因子。因此 $(x', y')=(1)$。经同样的计算，可得

$$(x', z')=(y', z')=(1).$$

(3)式可以重新写成

(4) $$x'y'z'=-\mu\lambda^{3(s-1)}v^3,\quad s-1\geqslant 1.$$

又容易看出

(5) $$x'+y'+z'=0.$$

因为 x', y', z' 无公因子，所以，从(4)式立得

(6) $$x'=\mu_1 x_1^3,\quad y'=\mu_2 y_1^3,\quad z'=\mu_3' z_1^3,$$

此处 μ_1, μ_2, μ_3' 是可逆元。又知 λ 整除 x', y', z' 之一，不妨设 $\lambda \mid z'$，由(4)式即知

$$z'=\mu_3\lambda^{3(s-1)}v_1,$$

这里 μ_3 是可逆元，$\lambda \nmid v_1$。代入(5)式，立得

(7) $$\mu_1 x_1^3+\mu_2 y_1^3+\mu_3\lambda^{3(s-1)}v_1=0,$$

其中 $\quad s-1\geqslant 1,\quad x_1 y_1 v_1\neq 0,\quad \lambda\nmid x_1 y_1 v_1.$

(7)式与(2)式是十分类似的。我们不难证明 $\mu_1=\pm\mu_2$。事实上，把(7)式 mod λ^3，利用 $x_1, y_1\equiv \pm 1 \pmod{\lambda}$ 以及 μ_1, μ_2 都是可逆

元(即只能是$\pm 1, \pm\omega, \pm\omega^2$)，即可得出$\mu_1 = \pm\mu_2$。用$\mu_1$去除(7)式，立得

$$x_1^3 + (\pm y_1)^3 + \mu' \lambda^{3(s-1)} v_1^3 = 0. \tag{8}$$

此式与(2)式完全相同，即$x_1, \pm y_1, v_1$是形如(2)式的方程的又一组解，而且具有较少的不可分解的因子数目。这就是我们所要找的矛盾。

习　题

1. 设R是整环。如果对于R的每个极大理想$\mathfrak{m}$，$R_\mathfrak{m}$都是D.V.R.，且对每个非零元素$a \in R$，R中只有有限多个极大理想包含a，证明R是Dedekind整环。

2. 设D是Dedekind整环，$\mathfrak{a}$是D的非零理想。证明$D/\mathfrak{a}$中每个理想都是主理想。由此导出D的任一理想都可由至多两个元素生成。

3. 证明只有有限多个极大理想的Dedekind整环是P.I.D.。

4. 设R是局部整环，但不是域，其极大理想$\mathfrak{m}$是主理想，且

$$\bigcap_{n=1}^{\infty} \mathfrak{m}^n = \{0\}.$$

证明R是离散赋值环。

5. 设R是整环，举例说明R的分理想与其拟逆元的乘积不一定等于R。

6. 设R是诺德整环。证明：$\mathfrak{a}$是R的分理想$\Longleftrightarrow\mathfrak{a}$是有限$R$模。

7. 设R是一个整环，$\mathfrak{a}$是R的分理想，试证下述三条是等价的：

(1) $\mathfrak{a}$是可逆的；

(2) $\mathfrak{a}$是有限R模，并且对R的任一素理想$\mathfrak{p}$，都有$\mathfrak{a}R_\mathfrak{p}$可

逆；

(3) $\mathfrak{a}$ 是有限 R 模，并且对 R 的任一极大理想 $\mathfrak{m}$，都有 $\mathfrak{a}R_{\mathfrak{m}}$ 可逆。

8. 在本节例 1 中，将 $(\bar{x})$ 分解为素理想乘积。

9. 证明 $\boldsymbol{Z}[\sqrt{2}]$ 是整数封闭的。

10. 证明 $\boldsymbol{Z}[\sqrt{2}]$ 的因子类群为零。

11. 证明 $\boldsymbol{Z}[e^{2\pi i/5}]$ 是欧几里得环。

12. 设 D 为 Dedekind 整环，$\mathfrak{a},\mathfrak{b},\mathfrak{c}$ 为 D 的理想。证明

(1) $\mathfrak{a}\cap(\mathfrak{b}+\mathfrak{c})=(\mathfrak{a}\cap\mathfrak{b})+(\mathfrak{a}\cap\mathfrak{c})$；

(2) $\mathfrak{a}+(\mathfrak{b}\cap\mathfrak{c})=(\mathfrak{a}+\mathfrak{b})\cap(\mathfrak{a}+\mathfrak{c})$。

§2 整数扩充

代数数论中讨论的代数整数环 D 是 $\boldsymbol{Z}$ 在一个代数扩域 K 中的整数闭包。代数几何学中的一维正则多项式整环 $k[x_1,\cdots,x_n]$ 也是 $k[x_1]$ 在一个代数扩域 $k(x_1,\cdots,x_n)$ 中的整数闭包，此处 x_1 是一个变数。已知 $\boldsymbol{Z}$ 及 $k[x_1]$ 都是 Dedekind 整环。我们要说明 D 及 $k[x_1,\cdots,x_n]$ 也是 Dedekind 整环。不难看出，D 及 $k[x_1,\cdots,x_n]$ 都是一维的及正规的。我们仅须证明它们是诺德环。

我们先证明：

引理 1 设 D 是一个正规诺德整环，K 是它的比域，L 是 K 的一个有限可离扩域，S 是 D 在 L 中的整数闭包。那么，S 是一个有限 D 模。

证明 1) 设 $n=[L:K]$。又设 Ω 是 K 的一代数闭包。那么，存在 $\sigma_1,\cdots,\sigma_n$: $L\to\Omega$ 是 n 个 K 嵌入。任取 $a\in L$，参考第五章 §8，有

$$\mathrm{Tr}_{L/K}(a)=\sum_i\sigma_i(a).$$

因此，如果 a 是对 D 整数相关的，那么，$\mathrm{Tr}_{L/K}(a)$ 也是对 D 整数

相关的，又在K中，所以$\mathrm{Tr}_{L/K}(a)\in D$。

2）任取L的一组K基$\{a_1,\cdots,a_n\}$。令a_i适合

$$\sum_{j=0}^{l} b_{ij}a_i^{l-j}=0,\qquad b_{ij}\in D.$$

那么，上式乘以b_{i0}^{l-1}以后，不难得出$b_{i0}a_i$是对D整数相关的。因此，存在L的一组K基$\{c_1,\cdots,c_n\}$，使得c_i对D皆为整数相关的。

3）任取$r\in S$，$r=\sum_i d_ic_i$，$d_i\in K$。令

$$d=\det[\mathrm{Tr}_{L/K}(c_ic_j)]\neq 0$$

（参见第五章§8定理5.33）。于是

$$D\ni\mathrm{Tr}_{L/K}(rc_j)=\mathrm{Tr}_{L/K}\left(\sum_i d_ic_ic_j\right)$$

$$=\sum_i d_i\mathrm{Tr}_{L/K}(c_ic_j),\quad j=1,\cdots,n.$$

由上面这一组线性方程式，可以解出d_i，

$$d_i\in d^{-1}D.$$

于是，$S\subset\sum_i(c_i/d)D=M$。M显然是一个有限D模，而D是诺德环，所以，S是有限D模。▎

系 S是诺德环。

当L不是K的可离扩域时，我们需要下面的引理。

引理2 设L是K的纯不可离扩域，p为K的特征，$L^{p^n}\subset K$。又设S是一个以L为其比域的Dedekind整环。那么，$S\cap K$也是一个Dedekind整环。

证明 令$q=p^n$，$D=S\cap K$。利用定理8.1，我们仅须证明D的非零理想I都是可逆的。已知SI是可逆的，因此存在$a_i\in I$，$s_i\in(SI)^{-1}=(S:SI)$，使

(1) $$\sum_i a_i s_i = 1.$$

q 是特征 p 的方幂，所以上式取 q 次方以后，得

(2) $$\sum_i a_i^q s_i^q = 1, \quad s_i^q \in L^q \subset K,$$

(3) $$\sum_i a_i a_i^{q-1} s_i^q = \sum_i a_i b_i = 1,$$

此处 $b_i = a_i^{q-1} s_i^q \in K$。我们又有 $b_i I \subset I^q s_i^q \subset S$，所以

$$b_i I \subset K \cap S = D,$$

也即 $b_i \in (D:I) = I^{-1}$。从(3)式立得

$$1 = \sum_i a_i b_i \in II^{-1},$$

即 $II^{-1} \supset D$，又显然 $II^{-1} \subset D$，所以 $II^{-1} = D$。▌

应用上面的引理，我们可以证明：

定理8.3 设 D 是 Dedekind 整环，K 是它的比域，L 是 K 的一个有限扩域，S 是 D 在 L 中的整数闭包。那么，S 也是一个 Dedekind 整环。

证明 设 L' 是 K 在 L 中的可离闭包，D' 是 D 在 L' 中的整数闭包。那么 D' 是一维正规环。应用引理1的系，D' 是诺德环。因此 D' 是 Dedekind 整环。

L 是 L' 的纯不可离扩域。根据第五章的定理5.20，存在一个 $q = p^t$，使 $L^q \subset L'$。令 Ω 是 L 的一个代数闭包，在 Ω 中取

$$L^* = (L')^{1/q} \supset L,$$

那么，映射

$$\sigma:\ L^* \to L', \quad x \mapsto x^q$$

是一个同构。令 $D^* = \sigma^{-1}(D')$。显然，D^* 也是一个 Dedekind整环。

我们要说明 $D^* \cap L = S$。如此，则由于$(L^*)^\sigma = L' \subset L$，应用引理 2，即得$S$是一个 Dedekind 整环。

任取 $a \in S$，令 $b = a^\sigma \in L'$。因为a是对D'整数相关的，所以b也对D'整数相关。而D'是整数封闭的，因此，$b \in D'$，即有

$$a \in \sigma^{-1}(D') = D^*, \qquad S \subset D^* \cap L.$$

反过来，任取 $c \in D^* \cap L$，则$c^\sigma \in D'$。于是c对D'是整数相关的，所以$c \in S$，即 $D^* \cap L \subset S$。▎

定义8.3 设L是$\mathbf{Q}$的一个有限扩域，D是$\mathbf{Z}$在L中的整数闭包。那么，称D为L的**代数整数环**。

定理8.4（古典理想理论） 在一个代数整数环D中，每一个理想I都可以唯一地分解成素理想的乘积。

证明 应用定理8.3及8.1。▎

设D是一个 Dedekind 整环，K是它的比域，$\mathfrak{p}$是D的一个素理想。设L是K的一个有限扩域，S是D在L中的整数闭包。那么，根据定理8.3，S也是一个 Dedekind 整环。因此，我们有

$$(*) \qquad \mathfrak{p}S = \prod_i \mathfrak{q}_i^{e_i}, \qquad \mathfrak{q}_i \neq \mathfrak{q}_j (i \neq j),$$

此处$\mathfrak{q}_i$是S的素理想。显然有$\mathfrak{q}_i \cap D \supset \mathfrak{p}$。而$\mathfrak{p}$是极大理想，$1 \notin \mathfrak{q}_i \cap D$，于是

$$\mathfrak{q}_i \cap D = \mathfrak{p}, \quad \forall i.$$

反之，设S的素理想$\mathfrak{q}$适合$\mathfrak{q} \cap D = \mathfrak{p}$，那么

$$\mathfrak{q} \supset \mathfrak{p}S = \prod_i \mathfrak{q}_i^{e_i},$$

于是，必有某个i，使$\mathfrak{q} \supset \mathfrak{q}_i$，即有$\mathfrak{q} = \mathfrak{q}_i$。

令v是与$\mathfrak{p}$相应的赋值，即$R_v = D_{\mathfrak{p}}$；w_i是与$\mathfrak{q}_i$相应的赋值，即$R_{w_i} = S_{\mathfrak{q}_i}$。那么

$$\mathfrak{m}_{w_i}\cap D=\mathfrak{m}_{w_i}\cap S\cap D=\mathfrak{q}_i\cap D=\mathfrak{p}.$$

所以 $$\mathfrak{m}_{w_i}\cap D_v=\mathfrak{p}D_v=\mathfrak{m}_v.$$

不难看出，w_i是 v 在 L 的一个扩充。根据(*)式，我们又有

$$\mathfrak{p}S_{\mathfrak{q}_i}=\mathfrak{q}_i^{e_i}S_{\mathfrak{q}_i}.$$

因此 v 的全序群 G_v对 w_i 的全序群 G_{w_i}的指数(即 w_i对 v 的缩分歧指数)为

$$[G_{w_i}:G_v]=e_i.$$

我们知道，

$$\Delta_{w_i}=R_{w_i}/\mathfrak{m}_{w_i}=S/\mathfrak{q}_i,\qquad \Delta_v=R_v/\mathfrak{m}_v=D/\mathfrak{p}.$$

所以，w_i对 v 的相对次数为

$$f_i=[\Delta_{w_i}:\Delta_v]=[S/\mathfrak{q}_i:D/\mathfrak{p}].$$

定义8.4 考虑上文，我们定义 $\mathfrak{q}_i$ **对** $\mathfrak{p}$ **的缩分歧指数**为w_i对 v 的缩分歧指数 e_i；$\mathfrak{q}_i$ **对** $\mathfrak{p}$ **的相对次数**(**或称剩余次数**) 为 w_i对 v 的相对次数 f_i。

我们立得下面的定理。

定理8.5 1) 设D是一个Dedekind 整环，K是它的比域，$\mathfrak{p}$是它的一个非零素理想。设L是K的一个有限扩域，S是D在L中的整数闭包(一个Dedekind整环)。令

$$\mathfrak{p}S=\prod_i\mathfrak{q}_i^{e_i},\qquad \mathfrak{q}_i\neq\mathfrak{q}_j\ (i\neq j).$$

那么 $$\sum_i e_if_i\leqslant[L:K],$$

这里 f_i 表示 $\mathfrak{q}_i$ 对 $\mathfrak{p}$ 的相对次数。

2) 更进一步，如果L是K的可离扩域，那么，我们有

$$\sum_i e_if_i=[L:K].$$

证明 应用定理7.15及定理7.19。 ∎

下面的定理将联系到域论中的伽罗瓦理论。

定理8.6 1）条件如同定理8.5的1)，又假设L是K的正规扩域。那么，所有的e_i都相等，令它是e；所有的f_i都相等，令它是f。又令$\mathfrak{q}_i$的个数是g。我们有$efg\leqslant[L:K]$。

2）更进一步，如果L是K的伽罗瓦扩域，则有

$$efg=[L:K]。$$

伽罗瓦群在$\{\mathfrak{q}_1,\mathfrak{q}_2,\cdots,\mathfrak{q}_g\}$上有传递性。

证明 令G是L的K自同构群。先证明G在$\{\mathfrak{q}_1,\mathfrak{q}_2,\cdots,\mathfrak{q}_g\}$上的作用是封闭的，而且有传递性。任取$\sigma\in G$。显然，如果$a\in S$，那么$a$对$D$整数相关，所以$\sigma(a)$对$D$也整数相关，$\sigma(a)\in S$，即有$\sigma(S)=S$。又知

$$\sigma(\mathfrak{q}_i)\cap D\supset\mathfrak{p},$$

所以$\sigma(\mathfrak{q}_i)\cap D=\mathfrak{p}$。显然$\sigma(\mathfrak{q}_i)$是$S$的素理想，按照定理8.4后面的讨论，$\sigma(\mathfrak{q}_i)\in\{\mathfrak{q}_1,\cdots,\mathfrak{q}_g\}$，即$\sigma$在$\{\mathfrak{q}_1,\cdots,\mathfrak{q}_g\}$上的作用是封闭的。现假设存在$\mathfrak{q}_j$不属于$\mathfrak{q}_1$的轨道

$$\mathrm{Orb}(\mathfrak{q}_1)=\{\mathfrak{q}_1,\cdots,\mathfrak{q}i\}。$$

那么，$\mathfrak{q}_j\not\subset\mathfrak{q}_1\cup\cdots\cup\mathfrak{q}_i$。取$a\in\mathfrak{q}_j\backslash(\mathfrak{q}_1\cup\cdots\cup\mathfrak{q}_i)$。不难看出，

$$\sigma_r(a)\overline{\in}\mathfrak{q}_1\cup\cdots\cup\mathfrak{q}_i\quad(\forall\sigma_r\in G)。$$

令$s=[L:\ K]/o(G)$，则

$$\left(\prod_{\sigma_r\in G}\sigma_r(a)\right)^s=\mathrm{N}_{L/K}(a)\in\mathfrak{q}_j\cap D=\mathfrak{p}\subset\mathfrak{q}_1,$$

所以必有某个r，使$\sigma_r(a)\in\mathfrak{q}_1$。这是自相矛盾的。因此，$G$作用在$\{\mathfrak{q}_1,\cdots,\mathfrak{q}_g\}$上是传递的。

由此易见，所有的e_i都相同，所有的f_i也都相同。本定理的其余部分，可以自定理8.5导出。▍

例5 我们现在来举一个例子(F.K.Schmidt)，说明定理8.5及定理7.15的不等式并不一定能由等式来代替。任何一个一秩离散赋值环R_v是一维正规诺德整环，因此是一个Dedekind整环。

令$\{z_0,z_1,\cdots,z_n,\cdots\}$是对$k_0=\boldsymbol{Z}/(p)$代数无关的。令

$$k=k_0(z_0,z_1,\cdots,z_n,\cdots),\quad K=k(x,y),$$

$$\varphi(x)=z_0^p+z_1^px^p+\cdots+z_n^px^{np}+\cdots\in k[[x]].$$

现在要说明σ：$k(x,y)\to k((x))$，$\sigma(x)=x$，$\sigma(y)=\varphi(x)$ 是嵌入。这就是说，$x,\varphi(x)$ 是代数无关的。假设$f(X,Y)\in k[X,Y]$是$x,\varphi(x)$适合的不可分解的多项式。令k_1 为 k_0 添加 f 的所有系数所得到的 k_0 的扩域。那么，k_1 是由 k_0 有限生成的域。因此有$f(X,Y)\in k_1[X,Y]$以及$\operatorname{tr}\deg(k_1/k_0)<\infty$。

显然，$X\nmid f(X,Y)$，即$f(0,Y)\neq 0$。已知$f(x,\varphi(x))=0$，故

$$f(0,\varphi(0))=f(0,z_0^p)=0.$$

所以，z_0 对 k_1 是代数相关的。令

$$f(X,X^pY+z_0^p)=X^tf_1(X,Y),\quad X\nmid f_1(X,Y),$$

那么$f_1(X,Y)\in k_1[X,Y]$，以及

$$f_1(x,z_1^p+\cdots+z_n^px^{(n-1)p}+\cdots)=0,$$

立得

$$f_1(0,z_1^p)=0.$$

所以z_1对k_1代数相关。以此类推，不难得出，k_0 上的代数无关集$\{z_0,\cdots,z_n,\cdots\}$中每个元素都对 k_1 代数相关。这是不可能的。所以，σ：$k(x,y)\to k((x))$是一个嵌入。

应用σ，一秩离散赋值环$R_u=k[[x]]$在$k(x,y)$上引生一个一秩离散赋值 v。不难看出，$G_v=G_u\approx\boldsymbol{Z}$，$\Delta_v=\Delta_u=k$。

我们现在要作一个纯不可离扩域

$$L=k(x,y)[y']=k(x,y'),$$

此处 $y'=y^{1/p}$。不难看出，v 在 L 上只有唯一的扩充 w，它是由

$$\sigma':\ k(x,y')\to k((x)),$$

$$\sigma'(x)=x,\quad \sigma'(y')=z_0+z_1x+\cdots+z_nx^n+\cdots$$

引生的。此时，$G_w=G_v\approx\boldsymbol{Z}$，$\Delta_w=\Delta_v=k$。所以

$$e=1,\quad f=1,\quad ef<p=[L:K].\ \blacksquare$$

设C是n维仿射空间的不可分解的曲线。这就是说，C的多项式函数环 $k[C]=k[x_1,\cdots,x_n]/\mathfrak{p}$是一维的整环，这里 $\mathfrak{p}=\mathscr{I}(C)$。又设$C$是无奇异点的曲线，则对 $k[C]$ 的任意素理想 $\mathfrak{q}$，$k[C]_\mathfrak{q}$

是正则局部环，应用定理6.45，它是唯一分解的整环，因此是正规环。于是，根据定理7.22，

$$k[C]=\bigcap k[C]_{\circ}$$

是一个正规环。这样，我们就证明了：

定理8.7 设$k[C]$是一个不可分解的、无奇异点的仿射曲线C的多项式函数环，那么，$k[C]$是一个Dedekind整环。

习　题

1. 设D是Dedekind整环，K是它的比域，L/K为有限扩张，S为D在L中的整数闭包，$\mathfrak{p}$为D的一个非零理想。证明$SD_{\mathfrak{p}}$为主理想整环。

2. 设R是主理想整环，K是它的比域，L/K是有限可离扩张，R在L中的整数闭包为S。证明S是自由R模，且

$$\mathrm{rank}_R S=[L:K].$$

3. 本习题(Kummer引理)给出一大类Dedekind环在扩充时素理想分解式的求法。

设D为Dedekind整环，K为D的比域，L/K是有限可离扩张，D在L中的整数闭包为S，且存在$\theta\in S$，使得$S=D[\theta]$。设θ适合K上的首一不可约多项式为$f(x)$。对于D的非零素理想$\mathfrak{p}$，设

$$f(x)(\bmod\ \mathfrak{p})=\bar{f}_1(x)^{e_1}\cdots\bar{f}_g(x)^{e_g},$$

其中$\bar{f}_i$均为$(D/\mathfrak{p})[x]$中首一不可约多项式，两两互异。证明

$$\mathfrak{p}S=\mathfrak{q}_1^{e_1}\cdots\mathfrak{q}_g^{e_g},$$

其中$\mathfrak{q}_i$皆为S中的素理想，$\mathfrak{q}_i=(f_i(\theta),\mathfrak{p})$，而$f_i(x)$是$D[x]$中的多项式，满足下列三个条件：(a) 首一；(b) $\deg f_i=\deg\bar{f}_i$；(c) $f_i(x)(\bmod\ \mathfrak{p})=\bar{f}_i(x)$。

4. 在$Q(\sqrt{-5})$中分解(3),(5),(7),(11)为素理想乘积。

5. 设$\zeta=\exp(2\pi i/15)$。将理想(3)和(5)在$Q(\zeta)$中分解为素理想的乘积。

6. 证明 $S=\boldsymbol{C}[x,y]/(x^2-y^3)$ 不是 Dedekind 整环，并画出 $x^2-y^3=0$ 的实图形．

7. 证明 $S=\boldsymbol{C}[x,y]/(x^2-y(y^2-1)(y^2-4)\cdots(y^2-g^2))$ 是一个Dedekind整环（其中 g 为正整数），并画出相应的实图形．

8. 符号如题7．在 S 中将理想 (x) 及 $(y-n)$ 分解为素理想的乘积（n 为整数）．

§3 判别式及表差式

在代数数论与代数几何学中，用到的Dedekind整环 D，都分别包含一个主理想整环 $\boldsymbol{Z}$ 或 $k[x]$，因此可以看成一个Dedekind整环的整数扩充．从Dedekind整环扩充的观点来看，有两个问题：一是求它在一个代数扩域中的整数闭包，另一个是考虑分歧点的问题．

我们先考虑第二个问题．设有两个Dedekind 整环 $D\subset S$．S 是 D 的整数扩充．任取 D 的一个素理想 $\mathfrak{p}$，令

$$\mathfrak{p}S=\prod_i \mathfrak{q}_i^{e_i}.$$

定义8.5 如果 $e_i=1$，且 $S/\mathfrak{q}_i$ 是 $D/\mathfrak{p}$ 的可离扩域，则称 $\mathfrak{q}_i$ 对 D 是**非分歧的**．如果所有的 $\mathfrak{q}_i$ 都是非分歧的，则称 $\mathfrak{p}$ 对 S 是**非分歧的**．

例 6 1）令 $S=\boldsymbol{C}[x,y]$，x,y 适合

$$y^2-x(x-1)(x-2)=0,$$

$D=\boldsymbol{C}[x]$．如果 $a\neq 0,1,2$，令 $\mathfrak{p}=(x-a)$，以及

$$\beta_1=\sqrt{a(a-1)(a-2)},\quad \beta_2=-\sqrt{a(a-1)(a-2)},$$

$$\mathfrak{q}_1=(x-a,y-\beta_1),\quad \mathfrak{q}_2=(x-a,y-\beta_2).$$

则

$$\mathfrak{p}S=\mathfrak{q}_1\mathfrak{q}_2.$$

这些 $\mathfrak{p},\mathfrak{q}_1,\mathfrak{q}_2$ 都是非分歧的．令 $b=0,1,2$．不难看出

$$(x-b)S=(x-b,y)^2.$$

所以，$(x-b)$，$(x-b,y)$ 都是分歧的．请看图8.2（见下页）．因为

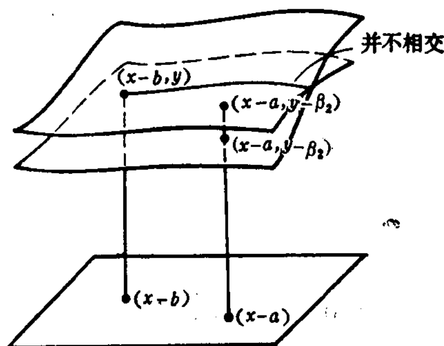


图 8.2

事实上这两个曲面不相交，所以在三维空间中无法作出图解，一定要到高维空间才行。

分歧点即是复叠映射的分支点。我们向 x 平面作复叠映射。在 x 平面上看，有三个点 $x=0,1,2$，其象源都不足两个点。它们上面有分支点 $(0,0),(1,0),(2,0)$。

2）令 $S=\boldsymbol{C}[x,y]$，x,y 适合

$$f(x,y)=y^2(y-1)-x^3-1=0.$$

应用代数几何学，不难看出，上面的方程式定义了无奇异点的曲线，因此 S 是一个Dedekind整环。令 $D=\boldsymbol{C}[x]$。不难看出

$$[\boldsymbol{C}(x,y):\boldsymbol{C}(x)]=3.$$

任取 D 的素理想 $\mathfrak{p}=(x-a)$，令

$$\mathfrak{p}S=\prod_i \mathfrak{q}_i^{e_i}.$$

应用定理8.5，我们有

$$\sum_i e_i f_i \leqslant [\boldsymbol{C}(x,y):\boldsymbol{C}(x)]=3.$$

考虑 $f(x,y)$ 的 y 判别式 $\mathrm{Dis}_y(f(x,y))$。经计算得出

$$\mathrm{Dis}_y(f(x,y)) = \begin{vmatrix} 1 & -1 & 0 & -x^3-1 & 0 \\ 0 & 1 & -1 & 0 & -x^3-1 \\ 3 & -2 & 0 & 0 & 0 \\ 0 & 3 & -2 & 0 & 0 \\ 0 & 0 & 3 & -2 & 0 \end{vmatrix}$$

$$= (27x^3+31)(x^3+1).$$

令$g(x)=\mathrm{Dis}_y(f(x,y))$。当$a$不适合$g(x)=0$时，$f(a,y)$有三个不同的根$\beta_1,\beta_2,\beta_3$。因此

$$(x-a)S = \prod_{i=1}^{3}(x-a, y-\beta_i).$$

于是$e_1=e_2=e_3=1$，$f_1=f_2=f_3=1$。因为$D/(x-a)=C$，其特征是零，所以定义8.5中的"可离扩域"的条件也适合了。因此，这些$\mathfrak{p}=(x-a)$都是非分歧的。

$g(x)=0$有六个解。我们试取$x=-1$来讨论。我们得出

$$(x+1)S=(x+1,y)^2(x+1,y-1).$$

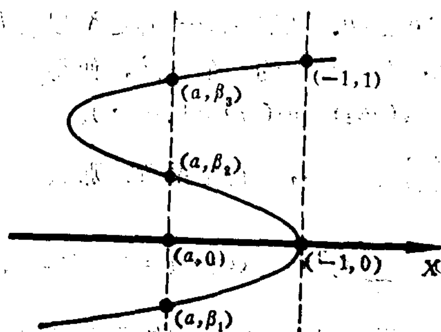


图 8.3

所以$(x+1,y)$是分歧的；$(x+1,y-1)$是非分歧的。我们无法作出图解。但是如果只考虑实数部分，可以作出如图8.3的示意图。

从另外的观点来看，

$$\mathrm{Dis}_y(f(x,y))=(f(x,y),f_y(x,y))=f_y(x,y)S$$

（因为在 S 里，$f(x,y)=0$），这也就是说，

$$g(x)S=(f_y(x,y))=(3y^2-2y)S. \quad \blacksquare$$

所以，我们通过计算$f_y(x,y)$便可得出分歧的理想。

为了叙述方便起见，先引入下面的定理，其证明留待以后再补。

定理8.8 设D是一个Dedekind整环，K是它的比域，L是K的一个有限可离扩域，S是D在L中的整数闭包。我们又设$S=D[y]$，$f(y)$是y对K的极小多项式。那么，$f'(y)$规定了S的所有的分歧理想，即S的素理想$\mathfrak{q}$是分歧的$\Longleftrightarrow\mathfrak{q}$是$f'(y)S$的素理想因子。

一般说来，$S=D[y]$的条件不能满足。Dedekind曾举出例子（见 Hasse 著《Number Theory》）。为了处理一般的情形，我们引入"互余模"的概念。

考虑L是K的一个有限可离扩域。那么，迹函数 $\mathrm{Tr}_{L/K}(a)$ 相当于内积。我们有下面的引理。

引理1 设$[L:K]=n$。任取 $a_1,\cdots,a_n\in K$ 以及L的一组K基$\{\omega_1,\cdots,\omega_n\}$，那么，存在唯一的一个$a\in L$，使得

$$\mathrm{Tr}_{L/K}(a\omega_i)=a_i(\forall i=1,\cdots,n).$$

证明 令$a=\sum\limits_j x_j\omega_j$，$x_j$是待定系数。那么

$$\mathrm{Tr}_{L/K}(a\omega_i)=\sum_j x_j\mathrm{Tr}_{L/K}(\omega_i\omega_j)=a_i \quad (i=1,\cdots,n)$$

是一组线性方程式。根据定理5.33，它的系数行列式

$$\det(\mathrm{Tr}_{L/K}(\omega_i\omega_j))\neq 0.$$

所以有唯一解。$\blacksquare$

应用上面的引理即知，任给L的一组基$\{\omega_1,\cdots,\omega_n\}$，都存在$L$的一组互余基$\{\omega_1',\cdots,\omega_n'\}$，使

$$\mathrm{Tr}_{L/K}(\omega_i\omega'_j)=\delta_{ij},$$

这里δ_{ij}是Kronecker 符号。互余基也即是**共轭基**。

设R是一个正规环，以K为比域，L是K的有限可离扩域。又设T是L的子集。那么，集合

$$T'=\{z\in L:\ \mathrm{Tr}_{L/K}(zT)\subset R\}$$

称为T对R的**互余集**。显然有

$$T_1\subset T_2 \Longrightarrow T'_1\supset T'_2.$$

当T是L的子环，而且T的比域是L时，则称T'是T对R的**互余模**。我们看几个例子。

例7 1）设$\{\omega_1,\cdots,\omega_n\}$是$L$的一组$K$基，$T=\sum_i R\omega_i$。任取$t'\in T'$，令

$$t'=\sum_i a_i\omega'_i,\quad a_i\in K,$$

其中$\{\omega'_1,\cdots,\omega'_n\}$是$L$的互余基。那么

$$a_j=\mathrm{Tr}_{L/K}(t'\omega_j)\in R.$$

由此不难看出，$T'=\sum_j R\omega'_j$，$(T')'=T$。

2）又设$\omega_i=a^{i-1}(i=1,\cdots,n)$，其余如上。令$a$对$K$的极小多项式为

$$f(x)=x^n+b_1x^{n-1}+\cdots+b_n=\prod_i(x-a_i),$$

其中$a_1=a$，a_i在L的一个代数闭包Ω中。应用内插法的公式，

$$\sum_{i=1}^n\frac{f(x)}{x-a_i}\frac{a_i^r}{f'(a_i)}=x^r,\quad r=0,1,\cdots,n-1.$$

上式又可以改写为

$$\mathrm{Tr}_{L/K}\left(\frac{f(x)}{x-a}\frac{a^r}{f'(a)}\right)=x^r,\quad r=0,1,\cdots,n-1. \tag{1}$$

我们研究$\frac{f(x)}{x-a}$。应用下面的计算

$$(2)\qquad \frac{f(x)}{x-a}=\frac{f(x)-f(a)}{x-a}=\sum_i b_i\frac{x^{n-i}-a^{n-i}}{x-a}$$

$$=\sum_i b_i(x^{n-i-1}+ax^{n-i-2}+\cdots+a^{n-i-1})$$

$$=c_0x^{n-1}+c_1x^{n-2}+\cdots+c_{n-1},$$

其中

$$(3)\qquad \begin{cases} c_0=b_0=1,\\ c_1=b_1+b_0a=b_1+a,\\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\ c_{n-1}=b_{n-1}+b_{n-2}a+\cdots+b_0a^n \end{cases}$$

以(2)式代入(1)式，比较两边的系数，立得

$$\mathrm{Tr}_{L/K}\left(\frac{c_{n-1-i}}{f'(a)}\cdot a^r\right)=\delta_{ir}.$$

因此
$$\left\{\frac{c_0}{f'(a)},\frac{c_1}{f'(a)},\cdots,\frac{c_{n-1}}{f'(a)}\right\}$$

是L的互余基。T的互余模$T'=\sum_i\frac{c_{n-i}}{f'(a)}R$。

3) 更进一步，设a对R是整数相关的。那么，$b_1,\cdots,b_n\in R$，所以

$$T'=\frac{1}{f'(a)}R+\frac{a}{f'(a)}R+\cdots+\frac{a^{n-1}}{f'(a)}R=\frac{1}{f'(a)}R,$$

此时$(T')^{-1}=f'(a)T$ ▌

定理8.9 设T，R如上。

1) T对R的互余模T'是T的一个分理想；

2) $(T')^{-1}$是T的一个非零理想。

证明 1) 如§2中引理1的证明。

2) $T'\supset T$。显然。 ▌

定义8.6 符号如上。$(T')^{-1}$称为T在R上的**表差式**（或**差**

积)，用符号$\mathscr{D}_{T/R}$表示之。

讨论 重新考虑定理8.8。应用例7的3)，我们知道

$$\mathscr{D}_{S/D}=f'(y)S.$$

那么，定理8.8无非是说，在$S=D[y]$时，$\mathscr{D}_{S/D}$规定了S的所有的分歧理想。下面，我们将对一般的情形证明这一点。▌

设R是Dedekind整环，T是R在L中的整数闭包。那么T也是Dedekind整环。于是，表差式$\mathscr{D}_{T/R}$可以写成T的素理想的乘积

$$\mathscr{D}_{T/R}=\prod_{\mathfrak{q}}\mathfrak{q}^{m(\mathfrak{q})}.$$

自然，除了有限多个素理想$\mathfrak{q}$之外，$m(\mathfrak{q})$皆为零。$m(\mathfrak{q})$称为$\mathfrak{q}$对R的**表差指数**。设$\mathfrak{p}=\mathfrak{q}\cap R$,

$$\mathfrak{p}T=\mathfrak{q}^{e(\mathfrak{q})}\prod_{i}\mathfrak{q}_i^{e(\mathfrak{q}_i)},\quad \mathfrak{q}_i\neq\mathfrak{q}.$$

那么，$e(\mathfrak{q})$是$\mathfrak{q}$的缩分歧指数。我们要比较$m(\mathfrak{q})$及$e(\mathfrak{q})-1$。请注意，$e(\mathfrak{q})>1$时，$\mathfrak{q}$是一个对R的分歧素理想。

我们先证明表差式可以局部化。见下定理。

定理8.10 设R是一个Dedekind整环，K是它的比域，L是K的一个有限可离扩域，T是R在L中的整数闭包。任取R的一个素理想$\mathfrak{p}$。令$M=R\backslash\mathfrak{p}$。以$R_M$及$T_M$分别表示$R$及$T$对分母系$M$的分式化，那么，

$$\mathscr{D}_{T/R}T_M=\mathscr{D}_{T_M/R_M}.$$

证明 显然，$R_M=R_\mathfrak{p}$也是一个Dedekind整环，T_M是它在L中的整数闭包。

$\subset$。任取$a=a'/m\in\mathscr{D}_{T/R}T_M$，此处$a'\in\mathscr{D}_{T/R}$，$m\in M$。再任取$T_M$对$R_M$的互余模$(T_M)'$的一个元素$b$。我们只须证明$ab\in T_M$便足够了。因为，这样就有

$$a\in((T_M)')^{-1}=\mathscr{D}_{T_M/R_M}.$$

已知$\mathrm{Tr}(bT_M)\subset R_M$。那么，$\mathrm{Tr}(bT)\subset R_M$。又已知$T$是一个

有限R模，所以$\mathrm{Tr}(bT)$的所有元素有一个公分母m_0。这就是说，

$$\mathrm{Tr}(m_0bT)=m_0\mathrm{Tr}(bT)\subset R.$$

换言之，$m_0b\in T'$，此处T'是T对R的互余模。应用a'的性质，立得$a'm_0b\in T$。所以

$$ab=(a'm_0b)/(mm_0)\in T_M.$$

$\supset$。任取$a\in\mathscr{D}_{T_M/R_M}$。再任取$b\in T'$（$T$对$R$的互余模）。显然

$$\mathrm{Tr}(bT_M)\subset R_M,$$

即$b\in(T_M)'$（T_M对R_M的互余模）。于是，$ab\in R_M$。现在我们在T'中变动b，即考虑

$$U=\{ab:\ b\in T'\}.$$

因为T'是一个有限R模，所以U也是一个有限R模。那么，U的所有元素有一个公分母m。这就是说，$mab\in R(\forall b\in T')$，也即

$$ma\in\mathscr{D}_{T/R},\quad a\in\mathscr{D}_{T/R}T_M. \blacksquare$$

系 设$\mathfrak{q}$在$\mathfrak{p}$之上（即$\mathfrak{q}\cap R=\mathfrak{p}$）。那么，$m(\mathfrak{q})$等于$\mathfrak{q}T_M$对$R_M$的表差指数。

为证明定理8.11，我们先证明下面的引理。

引理2 设R是Dedekind整环，K是它的比域，L是K的有限可离扩域，T是R在L中的整数闭包，令$\mathfrak{p}$是R的素理想，

$$\mathfrak{p}T=\prod_{i=1}^{g}\mathfrak{q}_i^{e_i}.$$

又令σ,σ_i为下面的典型映射

$$\sigma:\ R\to R/\mathfrak{p}=k,$$

$$\sigma_i:\ T\to T/\mathfrak{q}_i=k_i,\quad i=1,\cdots,g.$$

那么，对于$a\in T$，恒有

$$\sigma(\mathrm{Tr}_{L/K}(a))=\sum_{i=1}^{g}e_i\mathrm{Tr}_{k_i/k}(\sigma_i(a)).$$

证明 设$n=[L:K]=\sum_i e_if_i$，其中$f_i=[k_i:k]$（定理8.5）。

应用定理7.15的 1)的证明，我们可以选取L的K基

$$\{b_{is}c_{it}:\ i=1,\cdots,g,\ s=1,\cdots,e_i,\ t=1,\cdots,f_i\},$$

使

1) $b_{is}, c_{it}\in T(\Longrightarrow b_{is}c_{it}\in T)$;

2) $\{\sigma_i(c_{it}):\ t=1,\cdots,f_i\}$是$k_i$对$k$的基;

3) $\sigma_j(c_{it})=0,\ \forall j\neq i$;

4) $b_{is}\in \mathfrak{q}_i^{s-1}\backslash \mathfrak{q}_i^s$.

将基$\{b_{is}c_{it}\}$先按t，次按s，再按i的次序排好：

$$\{b_{11}c_{11}, b_{11}c_{12},\cdots,b_{11}c_{1f_1},b_{12}c_{11},\cdots,b_{12}c_{1f_1},\cdots b_{ge_g}c_{g1},\cdots,b_{ge_g}c_{gf_g}\}=\{\omega_1,\cdots,\omega_n\}.$$

令A为矩阵$[a_{ij}]_{n\times n}$，此处a_{ij}是如下定义的：

$$a\omega_i=\sum_{j=1}^{n}a_{ij}\omega_j.$$

那么，

$$\mathrm{Tr}_{L/K}(a)=\mathrm{Tr}A=\sum_i a_{ii}.$$

设

$$V_1=\sum_{l=1}^{e_1f_1}R\omega_l,\quad V_2=\sum_{l=f_1+1}^{e_1f_1}R\omega_l,\quad\cdots,$$

$$V_{e_1}=\sum_{l=(e_1-1)f_1+1}^{e_1f_1}R\omega_l,$$

$$V_{e_1+1}=\sum_{l=e_1f_1+1}^{e_1f_1+e_2f_2}R\omega_l,\quad\cdots,$$

$$V_{e_1+e_2}=\sum_{l=e_1f_1+(e_2-1)f_2+1}^{e_1f_1+e_2f_2}R\omega_l,\quad\cdots.$$

显然，$V_1\supset V_2\supset\cdots\supset V_{e_1}$，$V_{e_1+1}\supset V_{e_1+2}\supset\cdots\supset V_{e_1+e_2},\cdots$。现在我们考察

$$\sigma(\mathrm{Tr}_{L/K}(a))=\sigma(\sum a_{ii}).$$

为此，考虑映射

$$\bar{\sigma}: T \to T/\mathfrak{p}T.$$

自然，$T/\mathfrak{p}T$ 是 n 维 k 向量空间，它以$\{\bar{\sigma}(\omega_1),\cdots,\bar{\sigma}(\omega_n)\}$为一组基。令 $U_i=\bar{\sigma}(V_i)$，显然，U_i 是在 $\bar{\sigma}(A)$作用下的不变子空间，这里

$$\bar{\sigma}(A)=[\sigma(a_{ij})]_{n\times n}.$$

现取 $U_1\supset U_2\supset\cdots\supset U_{e_1}$ 来研究。不难看出，对于 $i=1,2,\cdots,e_1-1$，都有

$$U_i/U_{i+1}\approx\mathfrak{q}_1^{i-1}/\mathfrak{q}_1^i\approx T/\mathfrak{q}_1=k_1,$$

还有$U_{e_1}\approx k_1$。并且$\bar{\sigma}(A)$在它们上面的线性作用都等于 $\sigma_1(a)$在k向量空间 k_1 上的作用。因此，同样地考虑

$$U_{e_1+1}\supset U_{e_1+2}\supset\cdots\supset U_{e_1+e_2},\quad\cdots$$

之后，立得

$$\sigma(\mathrm{Tr}_{L/K}(a))=\sum_i e_i\mathrm{Tr}_{k_i/k}(\sigma_i(a)).\quad\blacksquare$$

定理8.11 设R 是 Dedekind 整环，K是它的比域，L 是K的有限可离扩域，T是R 在 L 中的整数闭包。任给T的素理想$\mathfrak{q}$，设

$$\mathfrak{q}\cap R=\mathfrak{p}.$$

令m 与 e 分别是 $\mathfrak{q}$ 对R 的表差指数及缩分歧指数。那么，我们恒有

$$m\geqslant e-1.$$

更进一步说，$m=e-1\Longleftrightarrow e$ 不是$R/\mathfrak{p}$的特征的倍数，并且$T/\mathfrak{q}$是$R/\mathfrak{p}$的可离扩域。

证明 应用定理8.10，我们可以局部化，即假设R 是一秩离散赋值环。设 $\mathfrak{p}=R\pi$。令

$$\mathfrak{p}T=T\pi=\prod_i\mathfrak{q}_i^{e_i},\qquad\mathscr{D}_{T/R}=\prod_i\mathfrak{q}_i^{m_i},$$

则 $T'=\prod_i\mathfrak{q}_i^{-m_i}$。所谓$m_i\geqslant e_i-1$，无非是说$\prod_i\mathfrak{q}_i^{1-e_i}\subset T'$。

任取 $a\in\prod_i \mathfrak{q}_i^{1-e_i}$，则 $a\pi\in\prod_i \mathfrak{q}_i$，$a\pi\in\mathfrak{q}_i(\forall i)$。令$N$是$K$的包含$L$的最小正规扩域。那么$a\pi$在$N$中的所有共轭元，必然也有同样的性质。由此不难导出

$$\mathrm{Tr}_{L/K}(a\pi)=\sum a\pi\text{的共轭元}\in\mathfrak{q}_i\cap R=\mathfrak{p},$$

也即

$$\pi\mathrm{Tr}_{L/K}(a)=\mathrm{Tr}_{L/K}(a\pi)\in R\pi,\qquad \mathrm{Tr}_{L/K}(a)\in R.$$

因为对于任给的 $a\in\prod_i \mathfrak{q}_i^{1-e_i}$，我们恒有$\mathrm{Tr}(a)\in R$，于是

$$\mathrm{Tr}_{L/K}(aT)\subset R,$$

即 $a\in T'$。至此定理的第一部分已证完。

现在我们证明定理的第二部分：

$\Longleftarrow$。因为$T/\mathfrak{q}$是$R/\mathfrak{p}$的可离扩域，所以存在 $\bar{b}\in T/\mathfrak{q}$，使

$$\mathrm{Tr}(\bar{b})\neq 0.$$

应用上面的讨论，令 $\mathfrak{q}=\mathfrak{q}_1$。由于 $\prod_{i>1}\mathfrak{q}_i^{e_i}$ 与 $\mathfrak{q}_1$ 是互为极大的 $\left(\text{即}\prod_{i>1}\mathfrak{q}_i^{e_i}+\mathfrak{q}_1=R\right)$，于是可以找到$\bar{b}$的象源 $b\in\prod_{i>1}\mathfrak{q}_i^{e_i}$。那么，应用上面的引理，即有

$$\sigma(\mathrm{Tr}_{L/K}(b))=e_1\mathrm{Tr}_{k_1/k}(\bar{b})\neq 0,$$

此处$k_1=T/\mathfrak{q}_1$，$k=R/\mathfrak{p}$。于是，$(b/\pi)\in\mathfrak{q}_1^{-e_1}$，$\mathrm{Tr}_{L/K}(b/\pi)\notin R$（为什么？）。所以$b/\pi\notin T'$。假若 $m_1\geqslant e_1$，则有

$$\mathfrak{q}_1^{-e_1}\subset\mathfrak{q}_1^{-m_1}\subset T'.$$

因此，从$b/\pi\in\mathfrak{q}^{-e_1}$，$b/\pi\notin T'$，立得$m_1=e_1-1$。

$\Longrightarrow$。假设e_1是$R/\mathfrak{p}(=k)$的特征的倍数，或者$T/\mathfrak{q}_1(=k_1)$是k的不可离扩域。令

$$\mathfrak{q}^*=\mathfrak{q}_1^{-e_1}\prod_{i>1}\mathfrak{q}_i^{1-e_i}.$$

任取 $c\in\mathfrak{q}^*$。那么 $c\pi\in\mathfrak{q}_i(\forall i>1)$。又用上面的引理，

$$\sigma(\mathrm{Tr}_{L/K}(c\pi))=e_1\mathrm{Tr}_{k_1/k}(\sigma_1(c\pi))=0.$$

所以 $\mathrm{Tr}_{L/K}(c\pi)\in R\pi$。故有

$$\pi\mathrm{Tr}_{L/K}(c)=\mathrm{Tr}_{L/K}(c\pi)\in R\pi,\quad \mathrm{Tr}_{L/K}(c)\in R,$$

那么，$\mathrm{Tr}_{L/K}(cT)\subset R(\forall c\in\mathfrak{q}^*)$，所以$\mathfrak{q}^*\subset T'$，即有$m_1\geq e_1$。▌

定理8.12 T的素理想$\mathfrak{q}$对R是分歧的$\Longleftrightarrow\mathfrak{q}\mid\mathscr{D}_{L/K}$。

证明 应用上定理，立得。▌

系 定理8.8。

证明 见定义8.6后面的讨论。▌

从定理8.12中，我们立刻得知只有有限多个$\mathfrak{q}\in T$是分歧的。在黎曼曲面论中，有更精确的 Hurwitz 公式：

$$2g_{C_1}-2=(2g_{C_2}-2)n+\sum_{\mathfrak{p}}(e(\mathfrak{p})-1),$$

此处，n 是黎曼曲面C_1对C_2的复叠次数，$g_{C_i}(i=1,2)$是C_i的亏格。

定理8.12告诉我们T中对R分歧的素理想$\mathfrak{q}$的分布情形。但是，R的分歧的素理想$\mathfrak{p}=\mathfrak{q}\cap R$的分布情形呢？固然，我们可以先求$\mathscr{D}_{T/R}$，再把$\mathscr{D}_{T/R}$的素理想因子$\mathfrak{q}$与$R$相交以得出$\mathfrak{p}$。这种方法繁复不便。我们要用判别式的方法来解决这个问题。

现在返回来研究定理8.8。那是一个比较简单的情形。在一个代数封闭域Ω里，求首一多项式$f(x)$的分解式

$$f(x)=\prod_{i=1}^{n}(x-y_i),\quad y=y_1,$$

那么，$f'(y_1)=\prod_{i>1}(y_1-y_i)$。而$f(x)$的判别式为

$$\mathrm{Dis}_x f(x)=\prod_{j=1}^{n}\Big(\prod_{i\neq j}(y_j-y_i)\Big)=\mathrm{N}_{L/K}(f'(y_1)).$$

从这个例子中，我们不难看出，检查重根的判别式$\mathrm{Dis}_x f(x)$与表

差式（在这里是$f'(y_1)$的范数）有密切的关系。这是我们要探明的。

相对于几何学而言，范数的作用相当于投影，而且照顾到代数重数。因此，自然的，我们对于理想$I\subset T$，也定义它的"范理想"（对应到R所规定的代数多样体的点集）如下：

定义8.7 设$I=\prod \mathfrak{q}_i^{n_i}$是$T$的理想。那么，$I$的**范理想**定义为

$$N_{L/K}(I)=\prod (\mathfrak{q}_i\cap R)^{n_i f_i},$$

此处f_i是$\mathfrak{q}_i$对R的剩余次数（即相对次数）。

讨论 不难看出，映射$N_{L/K}$具有下列的性质：

1) $N_{L/K}(I\cdot J)=N_{L/K}(I)\cdot N_{L/K}(J)$，$I\subset J\Longrightarrow N_{L/K}(I)\subset N_{L/K}(J)$；

2) 当$K\subset L\subset F$时，$N_{L/K}(N_{F/L}(I))=N_{F/K}(I)$；

3) 令I是R的理想，$n=[L:K]$，那么，$N_{L/K}(T\cdot I)=I^n$。

上面的性质3)是说，任取点集（对应于I），先找出此点集在映射$N_{L/K}$下的象源(对应于$T\cdot I$，一般言之，每个点都有n个点为象源)，再投影下来，此点集的重数将增加到n倍。此结论的证法如下：我们仅须考虑I是素理想$\mathfrak{p}$的情形。那么，只要利用$\sum_i e_i f_i=n$便可以得出结论了。▌

我们现在证明两个引理。

引理3 任取$a\in T$。那么$N_{L/K}(Ta)=RN_{L/K}(a)$。

证明 请注意，$N_{L/K}$对理想Ta及对元素a是分别定义的。这个引理是要说明这两个定义是一致的。以下分两个步骤来证明。

1) 假定L是K的伽罗瓦扩域，G是伽罗瓦群。我们用下面的符号：

$$Ta=\prod_{\mathfrak{q}} \mathfrak{q}^{v(\mathfrak{q},a)}.$$

考虑
$$TN_{L/K}(a)=\prod_{\mathfrak{q}} \mathfrak{q}^{v(\mathfrak{q},N(a))}.$$

因为 $$\mathrm{N}(a)(=\mathrm{N}_{L/K}(a))=\prod_{\sigma\in G}\sigma(a),$$

所以

$$v(\mathfrak{q},\mathrm{N}(a))=\sum_{\sigma\in G}v(\mathfrak{q},\sigma(a))=\sum_{\sigma\in G}v(\sigma^{-1}(\mathfrak{q}),a).$$

应用定理8.7，在上式中，每一个$\sigma^{-1}(\mathfrak{q})$都出现 ef 次，而且一共有 g 个不同的$\sigma^{-1}(\mathfrak{q})$(即$\mathfrak{q}_1,\cdots,\mathfrak{q}_g$)。因此上式可以缩写成

$$v(\mathfrak{q},\mathrm{N}(a))=ef\sum_{i=1}^{g}v(\mathfrak{q}_i,a).$$

现在考虑在R中的分解式，用下面的符号

$$Rb=\prod_{\mathfrak{p}}\mathfrak{p}^{u(\mathfrak{p},b)},\qquad b\in R.$$

令 $\mathfrak{p}=\mathfrak{q}\cap R$，$b=\mathrm{N}(a)$。那么

$$\mathfrak{p}=\prod_{\mathfrak{q}_i\cap R=\mathfrak{p}}\mathfrak{q}_i^{e}.$$

比较上面三式，不难得出 $u(\mathfrak{p},\mathrm{N}(a))=\sum fv(\mathfrak{q}_i,a)$。从而

$$\mathrm{N}(Ta)=\prod_{\mathfrak{q}}(\mathfrak{q}\cap R)^{v(\mathfrak{q},a)f}=\prod_{\mathfrak{p}}\prod_{\mathfrak{q}\cap R=\mathfrak{p}}(\mathfrak{q}\cap R)^{v(\mathfrak{q},a)f}$$

$$=\prod_{\mathfrak{p}}\mathfrak{p}^{\sum fv(\mathfrak{q}_i,a)}=R\mathrm{N}(a).$$

2) 在一般情形下，令 L^* 是K的包含L的最小伽罗瓦扩域，T^*是R在L^*中的整数闭包。那么，L^*也是L的伽罗瓦扩域。因此我们可以用1)以及上面定义8.7后面的讨论中的1)，2)，3)。

令 $n=[L:K]$，$m=[L^*:L]$。那么

$$\begin{aligned}(\mathrm{N}_{L/K}(Ta))^m&=\mathrm{N}_{L/K}(Ta)^m &&\text{(公式 1))}\\&=\mathrm{N}_{L/K}(\mathrm{N}_{L^*/L}(T^*a)) &&\text{(公式 3))}\\&=\mathrm{N}_{L^*/K}(T^*a) &&\text{(公式 2))}\end{aligned}$$

$$= R\mathrm{N}_{L^*/K}(a) \qquad \text{(步骤 1))}$$
$$= R\mathrm{N}_{L/K}(\mathrm{N}_{L^*/L}(a)) \qquad \text{(公式 2))}$$
$$= R\mathrm{N}_{L/K}(a^m) = R(\mathrm{N}_{L/K}(a))^m.$$

利用 Dedekind 整环的理想的唯一分解定理，立得本引理。 ∎

下面的引理 4 进一步阐明了 $\mathrm{N}_{L/K}$ 对理想及元素的两个定义是一致的。

引理 4 理想 $\mathrm{N}_{L/K}(I)$ 是由 I 的元素的范数生成的，即是由

$$\{\mathrm{N}_{L/K}(a) : a \in I\}$$

生成的理想。

证明 因为 $(a) \subset I$，由引理 3，显然有

$$(\mathrm{N}(a)) = \mathrm{N}((a)) \subset \mathrm{N}(I),$$

所以 $\mathrm{N}(I)$ 包含 $\{\mathrm{N}(a) : a \in I\}$ 所生成的理想 J。令 $I = \prod_i \mathfrak{q}_i^{n_i}$，则

$$\mathrm{N}(I) = \prod_{\mathfrak{p} = \mathfrak{q}_i \cap R} \mathfrak{p}^{\Sigma f(\mathfrak{q}_i) n_i} = \prod_{\mathfrak{p}_j | I} \mathfrak{p}_j^{l_j},$$

其中

$$l_j = \sum_{\mathfrak{q}_i | \mathfrak{p}_j T} f(\mathfrak{q}_i) n_i.$$

再令

$$J = \prod_{\mathfrak{p}_j} \mathfrak{p}_j^{m_j}.$$

我们已经说明了 $l_j \leqslant m_j$。现在只要证明：任给一个 $\mathfrak{p}_j$，必有一个 $a \in I$，使

$$\mathrm{N}(a) \in \mathfrak{p}_j^{l_j} \backslash \mathfrak{p}_j^{l_j+1}.$$

因为这样我们即可得出

$$\mathrm{N}(a) \subset J \implies l_j \geqslant m_j.$$

应用引理 1，我们只要找到 $a \in I$，使

$$a \in \mathfrak{q}_i^{n_i} \backslash \mathfrak{q}_i^{n_i+1}, \quad \forall \mathfrak{q}_i \cap R = \mathfrak{p}_j.$$

简而言之，因为 $a \in I \Longrightarrow a \in \mathfrak{q}_i^{n_i}$，所以即是求 $a \in I$，使

$$a \in \mathfrak{q}_i^{n_i+1}, \quad \forall \mathfrak{q}_i \cap R = \mathfrak{p}_j.$$

用T的理想唯一分解的性质，知

$$I \supsetneqq \prod_{\mathfrak{q}_i \cap R = \mathfrak{p}_j} \mathfrak{q}_i^{n_i+1},$$

所以可以找到这样的a。▎

我们定义T对R的“判别式”如下。

定义8.8 令T对R的表差式是$\mathscr{D}_{T/R}$。那么，T对R的判别式定义为

$$\delta_{T/R} = \mathrm{N}_{L/K}(\mathscr{D}_{T/R}).$$

讨论 从上面的定义，立得判别式$\delta_{T/R}$规定了R的分歧理想。下面的定理将说明，如此定义的判别式$\delta_{T/R}$与第五章§8定义的域判别式

$$\det[\mathrm{Tr}_{L/K}(u_i u_j)] = \mathrm{Dis}(u_1, \cdots, u_n)$$

的关系，从而提供了直接计算$\delta_{T/R}$的方法。

定理8.13 符号如上．任取L在T中的一组K基$\{u_1, \cdots, u_n\}$。令$d(u) = \mathrm{Dis}(u_1, \cdots, u_n)$。那么

1) $\delta_{T/R}$是由所有的$d(u)$生成的理想；

2) $\delta_{T/R} = R \cdot d(u) \Longleftrightarrow \{u_1, \cdots, u_n\}$是$T$的一组$R$基。

证明 1) 令J为由所有的$d(u)$生成的理想。本定理是要比较理想$\delta_{T/R}$, J及$R \cdot d(u)$。应用R是Dedekind整环的性质，我们仅须研究它们对任意一素理想$\mathfrak{p}$的指数。已知表差式$\mathscr{D}_{T/R}$可以局部化(定理8.10)，那么，显然的，$\delta_{T/R}$也可以局部化。为了书写方便起见，我们令$\delta = \delta_{T/R}$。

任取R的一个素理想$\mathfrak{p}$，令$M = R \backslash \mathfrak{p}$。我们现在考虑$R_M$($= R_\mathfrak{p}$), T_M, δ_M($= \delta R_M$)等。已知R_M是一个一秩离散赋值环，所以是一个主理想整环。易见T_M是主理想整环R_M的有限生成模。因此，根据第四章，有$\{u_1, \cdots, u_n\} \subset T_M$，使

$$T_M = \bigoplus_{i=1}^{n} R_M u_i,$$

自然，$\{u_1,\cdots,u_n\}$是L对K的一组基。取它的互余基$\{v_1,\cdots,v_n\}$，即

$$\mathrm{Tr}_{L/K}(u_i v_j)=\delta_{ij}.$$

那么，$\{v_1,\cdots,v_n\}$即是T_M对R_M的互余模$(T_M)'$的一组R_M基，即

$$(T_M)'=\bigoplus_{j=1}^{n} R_M\cdot v_j.$$

又因为T_M只有有限多个素理想，根据本章§1的习题3，T_M也是一个主理想整环。那么，$(T_M)'$作为T_M的一个分理想，是由一个元素$b\in L$生成的，即$(T_M)'=T_M\cdot b$。因此

$$\{bu_1,\cdots,bu_n\}$$

是$(T_M)'$对R_M的一组基。计算这组基的判别式，令$c^{(\alpha)}$表示c在L的一个代数闭包Ω中的共轭元素，

$$d(bu_1,\cdots,bu_n)=\det[\mathrm{Tr}_{L/K}(bu_i bu_j)]$$

$$=\det\left[\sum_{\alpha=1}^{n}(bu_i)^{(\alpha)}(bu_j)^{(\alpha)}\right]$$

$$=\det\begin{bmatrix}(bu_1)^{(1)} & \cdots & (bu_n)^{(1)}\\ \cdots & \cdots & \cdots\\ (bu_1)^{(n)} & \cdots & (bu_n)^{(n)}\end{bmatrix}^2$$

$$=\det\begin{bmatrix}b^{(1)} & & 0\\ & b^{(2)} & \\ 0 & & \ddots \ \ b^{(n)}\end{bmatrix}^2$$

$$\times\det\begin{bmatrix}u_1^{(1)} & \cdots & u_n^{(1)}\\ \cdots & \cdots & \cdots\\ u_1^{(n)} & \cdots & u_n^{(n)}\end{bmatrix}^2$$

$$=\mathrm{N}(b)^2 d(u).$$

考虑$(T_M)'$的两组基$\{v_1,\cdots,v_n\}$及$\{bu_1,\cdots,bu_n\}$的关系式，立刻

可以导出 $N(b)^2d(u)/d(v)$ 是 R_M 的可逆元。又，因为 v 是 u 的互余基，我们自然有 $d(u)d(v)=1$。所以

$$(N(b)d(u))^2=N(b)^2d(u)/d(v)$$

是 R_M 的可逆元。因此 $N(b)d(u)$ 必是 R_M 的可逆元。于是

$$N(b)^{-1}R_M=d(u)R_M.$$

我们知道(见引理 4) δ_M 是由 $\mathscr{D}_M(=\mathscr{D}_{T/R}T_M=\mathscr{D}_{T_M/R_M})$ 的所有元素 a 的范数 $N(a)$ 生成的。又知

$$a\in\mathscr{D}_M\Longleftrightarrow aT'_M\subset T_M\Longleftrightarrow ab\in T_M.$$

由此立得

$$\delta_M=N(b)^{-1}R_M=d(u)R_M.$$

现在我们任取 L 对 K 的基 $\{u'_1,\cdots,u'_n\}$，此处 $u'_i\in T$。那么，它的判别式 $d(u')$ 在 R_M 中是 $d(u)$ 的倍数。因此，对任给的素理想 $\mathfrak{p}$ 而言(有相应的 $M=R\backslash\mathfrak{p}$ 及相应的 $\{u_1,\cdots,u_n\}$)，总有

$$d(u')\in d(u)R_M=\delta_M.$$

那么，考虑 $\mathfrak{p}$ 的指数，立得 $d(u')\in\delta$，所以 $J\subset\delta$。

我们现在要证明 δ 是由所有 $d(u')$ 生成的。对于上述的 $\{u_1,\cdots,u_n\}$，乘以 R_M 的可逆元素，可以消去分母。故不妨令 $u_i\in T$ $(\forall i)$。此时 $d(u)\in R$，且它的 $\mathfrak{p}$ 的指数 $=\delta$ 的 $\mathfrak{p}$ 的指数，因此，

$$J\text{ 的 }\mathfrak{p}\text{ 的指数}\leqslant\delta\text{ 的 }\mathfrak{p}\text{ 的指数},$$

即 $J\supset\delta$。上面又已证过 $J\subset\delta$，所以 $J=\delta$。

2) $\Longleftarrow$。在给出的条件下，$\{u_1,\cdots,u_n\}$ 显然是 T_M 对 R_M 的一组基。上面已证 $d(u)R_M=\delta_M$，此式对任意 $\mathfrak{p}$ 都成立，所以立得

$$d(u)R=\delta.$$

$\Longrightarrow$。设 $\delta=d(u)R$。考虑对任给的素理想 $\mathfrak{p}$ 取局部化如上，则 $\delta_M=d(u)R_M$，此处 $M=R\backslash\mathfrak{p}$。任取 T_M 对 R_M 的一组基 $\{u''_1,\cdots,u''_n\}$。考虑它与 $\{u_1,\cdots,u_n\}$ 的关系式，不难导出 $\{u_1,\cdots,u_n\}$ 是 T_M 对 R_M 的一组基。现在要证明 $\{u_1,\cdots,u_n\}$ 是 T 对 R 的基。

任取 $a\in T$，可以写成

$$a = \sum_i a_i u_i, \quad a_i \in K.$$

在T_M中考虑上式，立得 $a_i \in R_M (= R_p)$。所以

$$a_i \in \bigcap R_M = \bigcap R_p = R. \quad \blacksquare$$

例 8 我们考虑$\boldsymbol{Q}$的二次扩域的代数整数环T。令 $L = \boldsymbol{Q}(\sqrt{m})$，$m \in \boldsymbol{Z}$，不妨令 m 没有重因子。于是$m \not\equiv 0 \pmod 4$。我们先计算T。

任取$a + b\sqrt{m} \in L$，$a, b \in \boldsymbol{Q}$。它的共轭元素是$a - b\sqrt{m}$。那么，$a + b\sqrt{m}$ 对$\boldsymbol{Z}$为整数相关的充要条件是：

$$(a + b\sqrt{m}) + (a - b\sqrt{m}) = 2a \in \boldsymbol{Z},$$

且

$$(a + b\sqrt{m})(a - b\sqrt{m}) = a^2 - b^2 m \in \boldsymbol{Z}.$$

不难导出，$a = a'/2$，$b = b'/2$，a'，$b' \in \boldsymbol{Z}$ 以及 $(a')^2 - (b')^2 m \equiv 0 \pmod 4$。因此有下面的结论：

1）如果$m \equiv 2, 3 \pmod 4$，则$a + b\sqrt{m} \in T \Longleftrightarrow a, b \in \boldsymbol{Z}$；

2）如果$m \equiv 1 \pmod 4$，则$a + b\sqrt{m} \in T \Longleftrightarrow a', b'$ 同时是奇数或偶数。

于是，T可以如下写出：

1）如果$m \equiv 2, 3 \pmod 4$，则$T = \boldsymbol{Z}[\sqrt{m}]$；

2）如果$m \equiv 1 \pmod 4$，则$T = \boldsymbol{Z}[(1 + \sqrt{m})/2]$。

应用定理8.8及8.13，立得

1）如果$m \equiv 2, 3 \pmod 4$，则表差式$\mathscr{D}_{T/Z} = 2\sqrt{m}T$，判别式 $\delta_{T/Z} = 4m\boldsymbol{Z}$；

2）如果$m \equiv 1 \pmod 4$，则表差式$\mathscr{D}_{T/Z} = \sqrt{m}T$，判别式$\delta_{T/Z} = m\boldsymbol{Z}$。

如果令$m = -1$，立得$2\boldsymbol{Z}$在扩域$\boldsymbol{Q}[\sqrt{-1}]$中是分歧的。参考第一章§5。

例 9 令 $p(\neq 2)$是一个素数。我们考虑割圆多项式

$$\varphi_p(x) = (x^p - 1)/(x - 1)$$

（参看第五章§6例7、例16的讨论）。令ζ是它的一个根。我们将证明$Z[\zeta]$即是$L=Q[\zeta]$的代数整数环T，并求其判别式及表差式。

已知$\varphi_p(x)=x^{p-1}+x^{p-2}+\cdots+x+1$是不可分解的，所以

$$[Q[\zeta]:Q]=p-1.$$

又知$\zeta\in T$，$\zeta-1\in T$，以及$\zeta-1$适合下面的方程式

$$F(x)=(x+1)^{p-1}+(x+1)^{p-2}+\cdots+1$$
$$=x^{p-1}+px^{p-2}+\cdots+p=0,$$

因此，$N_{L/Q}(\zeta-1)=p$。

我们又知

$$\varphi_p(x)=\prod_{i=1}^{p-1}(x-\zeta^i),$$

以$x=1$代入，得

$$p=\prod_{i=1}^{p-1}(1-\zeta^i).$$

任取i，j，我们可以求出$l_{ij}\in Z$，使$\zeta^i=(\zeta^j)^{l_{ij}}$（换句话说，$\zeta^i,\zeta^j$都是本原单位根）。那么，

$$(1-\zeta^i)/(1-\zeta^j)\in Z[\zeta]\subseteq T.$$

因此

$$p=(1-\zeta)^{p-1}\varepsilon,\quad \varepsilon\text{ 为 }T\text{ 的可逆元.}$$

考虑$N_{L/Q}(1-\zeta)=p$，立得$\mathfrak{q}=(1-\zeta)T$是一个素理想。在扩域L中，(p)的缩分歧指数$e=p-1(=[L:Q])$，所以$f=1$，$g=1$。

到此为止，我们还不知道T。为此现在我们来计算$\delta_{T/Z}$。再用定理8.13，求T及表差式$\mathscr{D}_{T/Z}$。

我们用局部化的方法：对p取局部化，$Z_{(p)}\subset T_{\mathfrak{q}}$，而且$(p)=\mathfrak{q}^{p-1}$。不难看出，一秩离散赋值环

$$T_{\mathfrak{q}}=Z_{(p)}+(1-\zeta)Z_{(p)}+\cdots+(1-\zeta)^{p-2}Z_{(p)}.$$

应用定理8.13，有

$$\delta_{T_{\mathfrak{q}}/Z_{(p)}}=(d(1,\zeta-1,\cdots,(\zeta-1)^{p-2}))$$

$$=\left(\prod_{i=1}^{p-1}F'(\zeta^{i}-1)\right)=\left(\prod_{i=1}^{p-1}\varphi_p'(\zeta^{i})\right)$$

$$=\left(\prod_{i=1}^{p-1}\frac{p(\zeta^{i})^{p-1}}{\zeta^{-i}-1}\right)=p^{p-2}\boldsymbol{Z}.$$

又在域扩张$Q[\zeta]/Q$下，考虑$d(1,\zeta-1,\cdots,(\zeta-1)^{p-2})$，自然也得同数$p^{p-2}$。根据定理8.13，$\delta_{T/\boldsymbol{Z}}|p^{p-2}\boldsymbol{Z}$。所以$\delta_{T/\boldsymbol{Z}}$没有别的素理想因子。那么，因为判别式$\delta_{T/\boldsymbol{Z}}$可以局部化，所以易于得出

$$\delta_{T/\boldsymbol{Z}}=p^{p-2}\boldsymbol{Z}.$$

再次应用定理8.13，立得$T=\boldsymbol{Z}[1-\zeta]=\boldsymbol{Z}[\zeta]$。

应用定理8.8，我们得出$\mathscr{D}_{T/\boldsymbol{Z}}=(\varphi_p'(\zeta))$。

例10 我们讨论不适合定理8.8的条件的情形。前文提过，Dedekind找出了数论的例子。现在我们就代数曲线论的范围来研究。已知在这个范围内，Dedekind整环T相当于无奇异点的仿射曲线C的多项式函数环。定理8.8的条件即是对适当选取的x,y而言，

$$T=\boldsymbol{C}[x,y]\supset\boldsymbol{C}[x].$$

换言之，C是一个平面曲线。那么，只要找出一个无法表现成仿射平面曲线的仿射空间曲线，便足以使定理8.8的条件不成立了。

我们可以取一个射影平面曲线$C\subset\boldsymbol{P}_{\boldsymbol{C}}^{2}$。选取$C$的一点$P$，使$P$不为任意典型因子(参见附录2)的零点集，即

$$(2g-2)P\neq K_0,$$

此处g是C的亏格，K是任取的典型因子。那么$C\backslash P$可以表现成一个仿射空间曲线，但是不能表现成仿射平面曲线。

具体一点，令C是由$x^4+(x-z)^4=y^4$定义的射影平面曲线。令

$$P=(a,1;0),$$

此处$a^4=1/2$。那么，C的亏格$g=3$，典型因子的零点集$K_0=$直线与C的交集。不难看出，没有直线l与C交于$(2\times3-2)P=4P$，

即没有直线 l 仅与 C 交于 P 点。这时，$C\backslash P$ 不能表示为仿射平面曲线，它的多项式函数环也因此不能写成 $\mathbf{C}[u,v]$。

请看代数几何学的专书，以了解这个例子。

习　题

1. 设 D 为 Dedekind 整环，K 为其比域，L/K 是有限可离扩张，D 在 L 中的整数闭包为 S，T 为 L 的子集，T' 为 T 对 D 的互余集。证明：

(1) 对 $a\in K^*$，$(aT)'=a^{-1}T'$；

(2) 若 $T\subset S$，则 $T\subset T'$；

(3) 若 T 为 L 的非零分理想，则 T' 亦是 L 的非零分理想。

2. 符号如题 1，证明

$$T'=\bigcap_{\mathfrak{p}\subset D}(D_{\mathfrak{p}}T')=\bigcap_{\mathfrak{p}\subset D}(D_{\mathfrak{p}}T)',$$

其中 $\mathfrak{p}$ 取遍 D 中的素理想，$(D_{\mathfrak{p}}T)'$ 表示 $D_{\mathfrak{p}}T$ 对 $D_{\mathfrak{p}}$ 的互余集。

3. 设 D 为 Dedekind 整环，K 为其比域，L/K 与 F/L 均为有限可离扩张，D 在 L 及 F 中的整数闭包分别为 S 和 R。证明：

$$\mathscr{D}_{R/D}=\mathscr{D}_{R/S}\cdot\mathscr{D}_{S/D},$$

其中 $\mathscr{D}$ 为表差式。

4. 符号如题 3。证明

$$\delta_{F/K}=(\delta_{L/K})^{[F:L]}\mathrm{N}_{L/K}(\delta_{F/L})$$

(δ 为判别式)。

5. 设 D 为 Dedekind 整环，K 为其比域，L/K，E/K 为有限可离扩张，且 L 和 E 在 K 的同一代数闭包内，D 在 L 及 E 中的整数闭包分别为 S 和 R，D 在 LE 中的整数闭包为 O，$L\cap E=K$，$(\delta_{S/D},\delta_{R/D})=(1)$。证明：

$$\delta_{O/D}=(\delta_{S/D})^{[E:K]}(\delta_{R/D})^{[L:K]}.$$

6. D,K,L,S 均如上题。设 $\mathfrak{p}$ 为 D 的一个非零素理想，$\mathfrak{p}$ 在 L 中有 r 个不同的素因子 $\mathfrak{q}_1,\mathfrak{q}_2,\cdots,\mathfrak{q}_r$，$\hat{D},\hat{K}$ 分别表示 D 和 K 在

$\mathfrak{p}$-adic拓扑下的完备化，$\hat{S}_i$和$\hat{L}_i$分别表示S和L在 $\mathfrak{q}_i$-adic 拓扑下的完备化。证明对S的任一理想$\mathfrak{a}$，有

$$\mathrm{N}_{L/K}(\mathfrak{a})\hat{D}=\prod_{i=1}^{r}\mathrm{N}_{\hat{L}_i/\hat{K}}(\mathfrak{a}\hat{S}_i).$$

7. 设D为Dedekind 环，K为D的比域，V是K上的n维向量空间。如果V的子集M适合条件：(a) M是有限D模；(b) M中含有V的一组K基，则称M是一个D格。证明：

(1) 对任一D格M，$M=\bigcap_{\mathfrak{p}\in \mathrm{Spec} D} D_{\mathfrak{p}}M$；

(2) 任给两个D格M和N，总有$a\in D$，使$aM\subset N$；

(3) 任给两个D格M和N，则对于几乎所有的$\mathfrak{p}\in \mathrm{Spec}D$，都有

$$D_{\mathfrak{p}}M=D_{\mathfrak{p}}N.$$

8. 设M,N是D格，且都是自由D模，M和N作为D模的基分别为$\{x_1,x_2,\cdots,x_n\}$和$\{y_1,y_2,\cdots,y_n\}$。再设

$$A\begin{bmatrix}x_1\\ \vdots\\ x_n\end{bmatrix}=\begin{bmatrix}y_1\\ \vdots\\ y_n\end{bmatrix},$$

其中A为K上的$n\times n$矩阵。则定义N对M的D模指数为$(\det A)D$，记为$[M:N]_D$。

若M和N不全是自由D模，则定义模指数为

$$[M:N]_D=\prod_{\mathfrak{p}\in \mathrm{Spec}D\setminus\{(0)\}}(\mathfrak{p}D_{\mathfrak{p}})^{v_{\mathfrak{p}}([D_{\mathfrak{p}}M:D_{\mathfrak{p}}N]_{D_{\mathfrak{p}}})}.$$

现设L/K为有限可离扩张，S为D在L中的整数闭包。证明：

(1) 对S中任一非零理想$\mathfrak{a}$(可视为D格)，有

$$\mathrm{N}_{L/K}(\mathfrak{a})=[S:\mathfrak{a}]_D.$$

(2) $\delta_{S/D}=[S':S]_D$，其中S'为S对D的互余模。

9. 设D,K,L,S,E,R,O均如题5。设$\mathfrak{p}$为D的一个素

理想，满足

$$\mathfrak{p}S = \mathfrak{q}^{[L:K]},$$

这里$\mathfrak{q}$是S中的素理想(此时称 $\mathfrak{p}$ 在S 中全分歧，参见第七章§5习题8)。又$\mathfrak{p}$在E中非分歧，$\mathfrak{m}$为E的一素理想，$\mathfrak{m} \cap S = \mathfrak{p}$。证明：

(1) $K = L \cap E$；

(2) $\mathfrak{q}$在LE中非分歧，$\mathfrak{m}$在LE中全分歧。

10．设$\zeta = \exp(2\pi i/p^n)$，这里 p 是奇素数。在 $\boldsymbol{Q}(\zeta)$ 中将(p)分解为素理想的乘积。

11．设 $\zeta = \exp(2\pi i/m)$，其中m为正整数，m 为奇数或$4|m$。证明：$p|m \Longleftrightarrow (p)$在$\boldsymbol{Q}(\zeta)$中分歧。

12．证明：$(2,\sqrt{10})$ 不是 $\boldsymbol{Z}[\sqrt{10}]$ 中的主理想。由此可知 $\boldsymbol{Z}[\sqrt{10}]$的因子类群不等于零。

13．设 $S = \boldsymbol{C}[x,y]/(x^2 - y(y-1))$。计算 $\delta_{S/C[x]}$。

14．设 $S = \boldsymbol{C}[x,y]/(x^2 - y(y^2-1))$。分别计算 $\mathscr{D}_{S/C[x]}$ 及 $\delta_{S/C[x]}$。

§ 4 分 歧 论

设D是一个 Dedekind 整环，K 是它的比域，L是K的有限可离扩域，S 是D在 L 中的整数闭包。在上一节中，我们已经证明了，D中只有有限多个素理想 $\mathfrak{p}_i$ 在S 中是分歧的。它们是由S 对D的判别式规定了的。同样，S 中只有有限多个素理想 $\mathfrak{q}_j$ 是对D分歧的。它们是由S 对D的表差式规定了的。在本节中，我们假定 L 是K 的伽罗瓦扩域，对一个特定的素理想 $\mathfrak{p} \subset D$，研究 $\mathfrak{p}$ 在S 中的分歧状况。

以下，令 $G = G(L/K)$，即为 L 对K 的伽罗瓦群。令 $\mathfrak{q}$ 是一个特定的在 $\mathfrak{p}$ 之上的素理想，即 $\mathfrak{q}$ 是 S 的素理想以及 $\mathfrak{q} \cap D = \mathfrak{p}$。

显然，G 作用在 $\mathfrak{q}$ 的共轭集$\{\mathfrak{q}_1, \cdots, \mathfrak{q}_g\}$(即是$S$的 所有 在 $\mathfrak{p}$ 之上的素理想的集合）上，此处 $\mathfrak{q}_1 = \mathfrak{q}$。应用定理8.6，$\mathfrak{q}$ 的轨道

$$\mathrm{Orb}(\mathfrak{q}) = \{\mathfrak{q}_1, \cdots, \mathfrak{q}_g\}.$$

我们有定义(参看第二章):

定义8.9 $\mathfrak{q}$ 的**分解群**定义为

$$G_Z = \{\sigma: \sigma(\mathfrak{q}) = \mathfrak{q}\} = \mathfrak{q} \text{ 的稳定子群 } \mathrm{Stab}(\mathfrak{q}).$$

讨论 1) 用第二章关于稳定子群的讨论，可知 G_Z 的阶

$$o(G_Z) = n/g = ef,$$

这里 $n = [L:K]$，e, f 分别为 $\mathfrak{q}$ 的缩分歧指数和剩余次数。

2) $\mathfrak{q}_i$ 的分解群 $= \sigma_i G_Z \sigma_i^{-1}$，即 G_Z 的共轭子群，此处 σ_i 满足

$$\mathfrak{q}_i = \sigma_i(\mathfrak{q}).$$

3) 德文"Zerlegung"是"分解"的意思，因此，我们用 G_Z 表示分解群。 ▎

令 K_Z 为 G_Z 的不变域。K_Z 称为 $\mathfrak{q}$ 的**分解域**. 应用伽罗瓦理论，立得 $L \supset K_Z \supset K$，L 是 K_Z 的伽罗瓦扩域，而且其伽罗瓦群

$$G(L/K_Z) \approx G_Z, \quad [L:K_Z] = ef, \quad [K_Z:K] = g.$$

令 D_Z 是 D 在 K_Z 中的整数闭包，$\mathfrak{q}_Z = \mathfrak{q} \cap D_Z$. 我们有下面的定理。

定理8.14 1) 我们有下面的关系式：$\mathfrak{q}_Z S = \mathfrak{q}^e$. 这就是说，$\mathfrak{q}$ 是 $\mathfrak{q}_Z$ 之上的唯一的素理想，而且 $\mathfrak{q}$ 对 D_Z 的缩分歧指数等于 $\mathfrak{q}$ 对 D 的缩分歧指数。自然的，$\mathfrak{q}$ 对 D_Z 的剩余次数 f 等于 $\mathfrak{q}$ 对 D 的剩余次数。

2) 更进一步说，如果 G_Z 是 G 的正规子群，那么，K_Z 自然是 K 的伽罗瓦扩域。此时

$$\mathfrak{p} D_Z = \prod_{i=1}^{g} (\mathfrak{q}_i)_Z, \quad (\mathfrak{q}_i)_Z = \mathfrak{q}_i \cap D_Z.$$

证明 1) 应用 G_Z 的定义，它的元素 σ 全部保持 $\mathfrak{q}$ 映到自身，因此，在 G_Z 作用下，$\mathrm{Orb}(\mathfrak{q}) = \{\mathfrak{q}\}$. 用定理8.6，立得 $\mathfrak{q}$ 是 $\mathfrak{q}_Z$ 之上的唯一的素理想，即

$$\mathfrak{q}_Z S = \mathfrak{q}^{e^*}.$$

我们现在要证明 $e = e^*$.

令 $f^*=[S/\mathfrak{q}:D_Z/\mathfrak{q}_Z]$。考虑 $D/\mathfrak{p}\subset D_Z/\mathfrak{q}_Z\subset S/\mathfrak{q}$，不难得出

$$f^*\leqslant f=[S/\mathfrak{q}:D/\mathfrak{p}].$$

显然，$\mathfrak{p}S=\mathfrak{p}D_ZS$，$\mathfrak{p}D_Z=\mathfrak{q}_Z^aI$，$a\geqslant 1$，$I$ 是 D_Z 的理想，从此立得

$$\mathfrak{q}^{ae^*}IS=\mathfrak{p}S=\mathfrak{q}^e\prod_{i>1}\mathfrak{q}_i^e.$$

由 Dedekind 整环的理想唯一分解定理，即知

$$ae^*\leqslant e\Longrightarrow e^*\leqslant e.$$

又显然 $e^*f^*=[L:K_Z]=ef$，结合前面已证的 $f^*\leqslant f$，立得

$$e=e^*,\quad f=f^*,\quad a=1.$$

2) 上面已证 $a=1$ 以及 $[D_Z/\mathfrak{q}_Z:D/\mathfrak{p}]=1$。从定理8.6立刻导出，$\mathfrak{q}_Z$ 在 K_Z 中有 g 个不同的共轭理想，以及

$$\mathfrak{p}D_Z=\prod_i(\mathfrak{q}_i)_Z.\quad \blacksquare$$

讨论 当 G 是交换群时，每一个子群都是正规子群。令

$$\mathfrak{p}S=\prod\mathfrak{q}_i^e.$$

因为 $\mathfrak{q}_i$ 的分解群是互相共轭的，所以在这种情形下，它们全相等。因此，G_Z,K_Z 是所有 $\mathfrak{q}_i$ 共有的。上定理说，在 K_Z 里，

$$\mathfrak{p}D_Z=\prod(\mathfrak{q}_i\cap D_Z),$$

即 $\mathfrak{p}D_Z$ 分解成 g 个不同的素理想。自然，每一个 $\mathfrak{q}_i\cap D_Z$ 对 D 的缩分歧指数及剩余次数都是 1。换句话说，从 K 到 K_Z 作域的扩充时，单纯而完全地表现了素理想 $\mathfrak{p}$ 的分解现象。$\blacksquare$

以下我们进一步求 K_Z 的扩域，以单纯而完全地表现素理想 $\mathfrak{q}$ 的剩余次数。我们给出定义：

定义8.10 令 $G_T=\{\sigma\in G:\sigma(a)\equiv a(\mathrm{mod}\ \mathfrak{q}),\ \forall a\in S\}$。称 G_T 为 $\mathfrak{q}$ 的**惯性群**。

讨论 1) 任取 $\sigma\in G_T$，$a\in\mathfrak{q}$。那么

$$\sigma(a)-a\equiv 0 \pmod{\mathfrak{q}},$$

即 $\sigma(a)\in\mathfrak{q}$。换句话说，$\sigma(\mathfrak{q})\subset\mathfrak{q}$。以 σ^{-1} 代入此式，又得

$$\mathfrak{q}\subset\sigma(\mathfrak{q})。$$

所以 $\sigma(\mathfrak{q})=\mathfrak{q}$。这也就是说 G_T 是 G_Z 的子群。

2）更进一步说，G_T 是 G_Z 的正规子群。任取 $\sigma\in G_T$，$\tau\in G_Z$，$a\in S$，则有

$$\tau\sigma\tau^{-1}(a)-a=\tau(\sigma\tau^{-1}(a)-\tau^{-1}(a))。$$

由于 $\sigma\tau^{-1}(a)-\tau^{-1}(a)\in\mathfrak{q}$，$\tau(\mathfrak{q})=\mathfrak{q}$，所以

$$\tau\sigma\tau^{-1}(a)-a\in\mathfrak{q}。$$

即 $\tau\sigma\tau^{-1}\in G_T$。

3）德文"Trägheit"是"惯性"的意思，所以我们用 G_T 表示惯性群。▌

令 K_T 表示 G_T 的不变域。K_T 称为 $\mathfrak{q}$ 的惯性域。用伽罗瓦理论，我们根据上面的讨论，即知

$$K\subset K_Z\subset K_T\subset L,$$

而且 L 对 K_T，K_T 对 K_Z 都是伽罗瓦扩域，它们的伽罗瓦群分别是 G_T 及 G_Z/G_T。令 D_T 是 D 在 K_T 中的整数闭包，$\mathfrak{q}_T=\mathfrak{q}\cap D_T$。我们有下面的定理：

定理8.15 1）$S/\mathfrak{q}$ 是 $D/\mathfrak{p}$ 的正规扩域，它的伽罗瓦群与 G_Z/G_T 同构；

2）令 L^* 为 $D/\mathfrak{p}$ 在 $S/\mathfrak{q}$ 中的可离闭包，$f_0=[L^*:D/\mathfrak{p}]$，p' 为 $D/\mathfrak{p}$ 的特征数，$[S/\mathfrak{q}:D/\mathfrak{p}]=f_0\cdot(p')^m$。那么，

$$[K_T:K_Z]=f_0,\quad \mathfrak{q}_Z D_T=\mathfrak{q}_T。$$

自然，$\mathfrak{q}_T$ 对 K_Z 的缩分歧指数是1，剩余次数是 f_0。

3）$[L:K_T]=e(p')^m$，$[S/\mathfrak{q}:D_T/\mathfrak{q}_T]=(p')^m$，$S/\mathfrak{q}$ 是 $D_T/\mathfrak{q}_T$ 的纯不可离扩域，$\mathfrak{q}_T D=\mathfrak{q}^e$。自然，$\mathfrak{q}$ 对 K_T 的缩分歧指数是 e，剩余次数是 $(p')^m$。

证明 1）及2）。任取 $\bar{a}\in S/\mathfrak{q}$，令 a 是 $\bar{a}$ 的象源。设 a 对 K 的极小多项式为

$$f(x)=x^n+c_1x^{n-1}+\cdots+c_n,\quad c_n\in D.$$

因为L是K的正规扩域，所以上式可以分解成

$$f(x)=\prod_{i=1}^{n}(x-a_i),\quad a_i\in S,\ a_1=a.$$

对$\mathfrak{q}$取剩余，立得

$$\bar{f}(x)=\prod_{i=1}^{n}(x-\bar{a}_i),\quad \bar{a}_1=\bar{a}.$$

因而$\bar{a}$对$D/\mathfrak{p}$的极小多项式必是$\bar{f}(x)$的因子，它在$S/\mathfrak{q}$中有所有的根。我们立刻导出$S/\mathfrak{q}$是$D/\mathfrak{p}$的正规扩域。

令$\bar{G}$为$S/\mathfrak{q}$对$D/\mathfrak{p}$的自同构群。我们定义由$\sigma\mapsto\bar{\sigma}$所引生的映射$G_Z/G_T\to\bar{G}$，这里

$$\bar{\sigma}(\bar{a})=\overline{\sigma(a)},\quad \sigma\in G_Z.$$

显然，这个定义与$\bar{a}$的象源a的选取无关。但

$$\bar{\sigma}\text{ 为幺映射}\Longleftrightarrow\sigma(a)-a\in\mathfrak{q}(\forall a\in S)\Longleftrightarrow\sigma\in G_T.$$

因此，这个映射的定义是良好的，而且是一个单射。

显然，$\bar{G}$是L^*对$D/\mathfrak{p}$的伽罗瓦群。应用定理5.21，L^*是$D/\mathfrak{p}$的一单扩域，故可设$L^*=(D/\mathfrak{p})[\bar{b}]$。任取$\sigma'\in\bar{G}$，我们要证明，存在一个$\sigma\in G$，使$\bar{\sigma}=\sigma'$。这样就建立了$G_Z/G_T$到$\bar{G}$的单满映射，因而不难看出，二者是同构的。要验证$\bar{\sigma}=\sigma'$，只要证明$\bar{\sigma}(\bar{b})=\sigma'(\bar{b})$即可。

令b是$\bar{b}$的象源。又令$b_j\in S$是b对于K_Z的共轭元素，这里$b_1=b$。那么，与前面一样，$\bar{b}$对于$D_Z/\mathfrak{q}_Z$的共轭元素不出$\{\bar{b}_1,\cdots,\bar{b}_j,\cdots\}$之外。我们应用定理8.14，不难导出

$$[D_Z/\mathfrak{q}_Z:D/\mathfrak{p}]=1,$$

即$D_Z/\mathfrak{q}_Z=D/\mathfrak{p}$。因此，$\bar{b}$对于$D/\mathfrak{p}$的共轭元素也不出$\{\bar{b}_1,\cdots,\bar{b}_j,\cdots\}$之外。于是$\sigma'(\bar{b})=\bar{b}_j$(对某个$j$)。自然有一个$\sigma\in G_Z$，使$\sigma(b)=b_j$。那么，$\sigma'=\bar{\sigma}$。这样就证明了1)。

这样，即有$[K_T:K_Z]=o(G_Z/G_T)=[L^*:D/\mathfrak{p}]=f_0$。我们把

上面的讨论，应用到 $K^*=K_T\subset L$ 的情形（即以 K^* 取代上面的 K）。那么，$K_Z^*=K_T^*=K^*$，相应的群 $G_Z^*=G_T^*=G^*$。于是

$$f_0^*=[K_T^*:K_Z^*]=1.$$

这就是说 $S/\mathfrak{q}$ 是 $D^*/\mathfrak{p}^*=D_T/\mathfrak{q}_T$ 的纯不可离扩域。换言之，

$$L^*\subset D_T/\mathfrak{q}_T,\quad [D_T/\mathfrak{q}_T:D/\mathfrak{q}]\geqslant f_0.$$

又从另外一方面来考虑，我们有

$$[D_T/\mathfrak{q}_T:D/\mathfrak{p}]\cdot e(\mathfrak{q}_T)\leqslant f_0,$$

其中 $e(\mathfrak{q}_T)$ 为 $\mathfrak{q}_T$ 对 K 的缩分歧指数。因此立得 $D_T/\mathfrak{q}_T=L^*$，

$$[D_T/\mathfrak{q}_T:D/\mathfrak{p}]=[D_T/\mathfrak{q}_T:D_Z/\mathfrak{q}_Z]=f_0,$$

$\mathfrak{q}_T$ 对 D_Z 的缩分歧指数等于 1，$\mathfrak{q}_Z D_T=\mathfrak{q}_T$。

3) 已经知道 $[L:K_Z]=ef=ef_0\cdot(p')^m$，$[K_T:K_Z]=f_0$，所以

$$[L:K_T]=e\cdot(p')^m.$$

显然，$\mathfrak{q}_T S=\mathfrak{q}^e$，那么，$\mathfrak{q}$ 对 K_T 的剩余次数必然是 $(p')^m$。▎

讨论 上面两个定理是说，从 K 到 L 的伽罗瓦扩张，可以插入两个扩域：从 K 到 K_Z，分开了 $\mathfrak{p}$ 上面的素理想 $\{\mathfrak{q}_Z\}$；任取出一个 $\mathfrak{q}_Z$，再从 K_Z 扩充到 K_T，此时单纯地显现了商域（或称剩余域）的可离扩张，$\mathfrak{q}_Z$ 并无分解现象，也无缩分歧指数的增加；从 K_T 扩充到 L，此时显现了缩分歧指数的全部增加，以及商域的纯不可离扩张。我们可以列出下表：

域扩张次数		g		f_0		$e\cdot(p')^m$	
域	K	$\subset$	K_Z	$\subset$	K_T	$\subset$	L
整环	D	$\subset$	D_Z	$\subset$	D_T	$\subset$	S
素理想	$\mathfrak{p}$	$\subset$	$\mathfrak{q}_Z$	$\subset$	$\mathfrak{q}_T$	$\subset$	$\mathfrak{q}$
剩余次数		1		f_0		$(p')^m$	
缩分歧指数		1		1		e	

定义8.11 应用上面的记号，我们定义 $\mathfrak{q}$ 对 D 的**分歧指数**为 $e\cdot(p')^m$。

例11 参考例 8。令 L 是 $\mathbf{Q}$ 的二次扩域，$L=\mathbf{Q}(\sqrt{m})$，$m\in$

$\boldsymbol{Z}$，m无重因子。那么，L显然是$\boldsymbol{Q}$的伽罗瓦扩域。令T是L的代数整数环。根据例 8 的计算，我们已知：

1）如果 $m\equiv 2,3(\bmod 4)$，则表差式$\mathscr{D}_{T/\boldsymbol{Z}}=2\sqrt{m}\,T$，判别式

$$\delta_{T/\boldsymbol{Z}}=4m\boldsymbol{Z};$$

2）如果 $m\equiv 1(\bmod 4)$，则表差式 $\mathscr{D}_{T/\boldsymbol{Z}}=\sqrt{m}\,T$，判别式

$$\delta_{T/\boldsymbol{Z}}=m\boldsymbol{Z}.$$

因此，我们立刻算出 $\boldsymbol{Z}$ 中对 L 分歧的素数如下：

1）p 是m的奇素因子；

2）如果 $m\equiv 2,3(\bmod 4)$，则 2 也是分歧素数。

在这种情形下，$pT=\mathfrak{q}^2T$。

我们考虑其余的素数 $p\nmid m$。

1）如果 $m\equiv 2,3(\bmod 4)$，则 $T=\boldsymbol{Z}+\boldsymbol{Z}\sqrt{m}$。令 $\mathfrak{q}$ 为 T 的素理想，$\mathfrak{q}\cap\boldsymbol{Z}=p\boldsymbol{Z}$。那么，令 $\sigma: \boldsymbol{Z}[x]\to T=\boldsymbol{Z}[\sqrt{m}]$为 $\sigma(x)=\sqrt{m}$引生的环映射，则

$$T/\mathfrak{q}\approx\boldsymbol{Z}[x]/\sigma^{-1}(\mathfrak{q})\approx((\boldsymbol{Z}/p\boldsymbol{Z})[x]/(x^2-\bar{m}))/\bar{\mathfrak{q}},$$

其中 $\bar{\mathfrak{q}}$ 为$\sigma^{-1}(\mathfrak{q})$在自然映射

$$\boldsymbol{Z}[x]\to(\boldsymbol{Z}/p\boldsymbol{Z})[x]\to(\boldsymbol{Z}/p\boldsymbol{Z})[x]/(x^2-\bar{m})$$

下的象。

如果方程式 $x^2-\bar{m}=0$ 在 $\boldsymbol{Z}/p\boldsymbol{Z}$ 中有解，则

$$(\boldsymbol{Z}/p\boldsymbol{Z})[x]/(x^2-\bar{m})\approx(\boldsymbol{Z}/p\boldsymbol{Z})\oplus(\boldsymbol{Z}/p\boldsymbol{Z}),$$

于是不难看出，$T/\mathfrak{q}=\boldsymbol{Z}/p\boldsymbol{Z}$，即 $f=[T/\mathfrak{q}:\boldsymbol{Z}/p\boldsymbol{Z}]=1$，$g=2$。所以

$$pT=\mathfrak{q}_1\mathfrak{q}_2,\qquad \mathfrak{q}_1\neq\mathfrak{q}_2.$$

我们称这种 p 为**分解型的**。请注意，上面的条件（$x^2-\bar{m}=0$ 在 $\boldsymbol{Z}/p\boldsymbol{Z}$ 中有解）即是 Legendre 符号$\left(\frac{m}{p}\right)=1$。

如果方程式 $x^2-\bar{m}=0$ 在 $\boldsymbol{Z}/p\boldsymbol{Z}$ 中无解，则不难看出

$$T/\mathfrak{q}=(\boldsymbol{Z}/p\boldsymbol{Z})[\sqrt{\bar{m}}],\quad [T/\mathfrak{q}:\boldsymbol{Z}/p\boldsymbol{Z}]=2,\quad g=1,$$

此时 $pT=\mathfrak{q}$。我们称这样的 p 为惯性型的。这时的条件即是 Legendre 符号 $\left(\frac{m}{p}\right)=-1$。

2) 如果 $m\equiv1 \pmod 4$，则奇素数的分解情况与 1)全同。但关于素数 2 的讨论并没有完成。令 $e^*=(1+\sqrt{m})/2$，那么 $T=\mathbf{Z}[e^*]$。e^* 对于 $\mathbf{Q}$ 的极小方程式是

$$x^2-x-(m-1)/4=0.$$

上式 mod 2 以后，当 $m\equiv1 \pmod 8$ 时，此方程式在 $(\mathbf{Z}/2\mathbf{Z})[x]$ 中可以分解。此时 2 是分解型的。当 $m\equiv5 \pmod 8$ 时，此方程式在 $\mathbf{Z}/2\mathbf{Z}$ 中无根，2 是惯性型的。

当 p 是分解型时，$K_Z=K_T=L$，$G_Z=G_T=\{e\}$；

当 p 是惯性型时，$K=K_Z, K_T=L, G_Z=\{e,\tau\}=G, G_T=\{e\}$；

当 p 是分歧型时，$K=K_Z=K_T$，$G_Z=G_T=G=\{e,\tau\}$，

上面的 τ 是由 $\sqrt{m}\mapsto-\sqrt{m}$ 引生出的 L 的自同构。

例12 参考例 9。令 p 是一个奇素数。我们考虑割圆多项式

$$\varphi_p(x)=(x^p-1)/(x-1).$$

令 ζ 是它的一个根。则 $\mathbf{Q}[\zeta]=L$ 的代数整数环 $T=\mathbf{Z}[\zeta]$。

我们经知道 $\delta_{T/\mathbf{Z}}=(p^{p-2})$，$\mathscr{D}_{T/\mathbf{Z}}=(\varphi_p'(\zeta))=((1-\zeta)^{p-2})$。因此，在有理素数中，$p$ 是唯一的分歧素数，

$$pT=(1-\zeta)^{p-1}T.$$

对 $(1-\zeta)$ 而言，$K=K_Z=K_T$。

任取一个素数 $p_1\neq p$。不难看出，它的缩分歧指数 $e=1$，而且因为 $\mathbf{Z}/p_1\mathbf{Z}$ 是完全域，所以，上面定理中的 $f_0=f$。

已知 L 对 $\mathbf{Q}$ 的伽罗瓦群 G 是循环群，$o(G)=p-1$，所以在 $m\mid p-1$ 时，它有唯一的 m 阶子群。因此，对一个固定的 p_1，想要决定 G_Z, G_T 等，无非是决定它们的阶。

已知 $p_1(\neq p)$ 是非分歧的，$e=1$，所以 $fg=p-1$。我们现在来计算 f。令 $\mathfrak{q}_1$ 是 T 的素理想，$\mathfrak{q}_1\cap\mathbf{Z}=p_1\mathbf{Z}$。令

$$\sigma: \mathbf{Z}[x]\to T=\mathbf{Z}[\zeta]$$

为 $\sigma(x)=\zeta$ 引生的环映射，则

$$T/\mathfrak{q}\approx \boldsymbol{Z}[x]/\sigma^{-1}(\mathfrak{q})\approx((\boldsymbol{Z}/p_1\boldsymbol{Z})[x]/(\overline{\varphi}_p(x)))/\overline{\mathfrak{q}},$$

其中 $\overline{\varphi}_p(x)$ 为 $\varphi_p(x)$ 在自然映射 $\boldsymbol{Z}[x]\to(\boldsymbol{Z}/p_1\boldsymbol{Z})[x]$ 下的象，$\overline{\mathfrak{q}}$ 为 $\sigma^{-1}(\mathfrak{q})$ 在映射 $\boldsymbol{Z}[x]\to(\boldsymbol{Z}/p_1\boldsymbol{Z})[x]\to(\boldsymbol{Z}/p_1\boldsymbol{Z})[x]/(\overline{\varphi}_p(x))$ 下的象。我们考虑 $(\boldsymbol{Z}/p_1\boldsymbol{Z})[x]/(\overline{\varphi}_p(x))$。易见

$$\overline{\varphi}_p(x)=\prod_{i=1}^{l}h_i(x),\quad h_i(x)\in(\boldsymbol{Z}/p_1\boldsymbol{Z})[x],$$

其中诸 $h_i(x)$ 是不可分解的多项式，而且两两不同(因为 $\overline{\varphi}_p(x)$ 无重根)，于是

$$(\boldsymbol{Z}/p_1\boldsymbol{Z})[x]/(\overline{\varphi}_p(x))\approx\bigoplus_{i=1}^{l}(\boldsymbol{Z}/p_1\boldsymbol{Z})[x]/(h_i(x))=\bigoplus_{i=1}^{l}k_i,$$

此处 k_i 都是域。于是，不难看出，$T/\mathfrak{q}$ 与某个 k_i 自然同构。注意到 $\varphi_p(x)$ 的每一个根都是 p 次本原单位根，应用伽罗瓦理论，可知诸 $h_i(x)$ 次数皆相等。令

$$f=\deg h_i(x),$$

则 f 即是 $\mathfrak{q}$ 对 Q 的剩余次数。易知 $l=g$。

现在我们要说明

$$f=\min\{f^*: f^* \text{为正整数},\ p_1^{f^*}\equiv 1 (\bmod p)\}.$$

这是因为，$h_i(x)$ 的任一个根 $\zeta_i(\neq 1)$，同时适合

$$\zeta_i^p=1,\quad \zeta_i^{p_1^f-1}=1,$$

所以 $p\mid p_1^f-1$；反之，设有 f^*，使 $p\mid p_1^{f^*}-1$。那么，

$$x^p-1\mid x^{p_1^{f^*}-1}-1,$$

所以 x^p-1 的根在基数为 $p_1^{f^*}$ 的有限域 k^* 中。立得 $h_i(x)$ 的根在 k^* 中，所以 $f\leqslant f^*$。

上面我们已经算出了 f。于是 $g=(p-1)/f$。这样，我们就可以知道 $G_Z(G_T=\{e\})$ 及 $K_Z(K_T=L=Q[\zeta])$。

习　题

1. 设D为Dedekind整环，K为其比域，L/K为有限伽罗瓦扩张，F为L/K的中间域，$H=G(L/F)$，$\mathfrak{q}$为L中的素理想，$\mathfrak{q}$关于L/K的分解群和惯性群分别为G_Z和G_T。证明：$\mathfrak{q}$关于L/F的分解群和惯性群分别为$G_Z \cap H$及$G_T \cap H$。

2. 设D为Dedekind整环，K为其比域，F/K为有限可离扩张，L是包含F的K上的最小伽罗瓦扩域，$\mathfrak{p}$是D的一个非零素理想。证明

(1) $\mathfrak{p}$在F内完全分裂$\Longleftrightarrow \mathfrak{p}$在$L$内完全分裂(所谓$\mathfrak{p}$在$F$内完全分裂(splits completely)，即$\mathfrak{p}$在F内分解为$[F:K]$个不同的素因子)；

(2) $\mathfrak{p}$在F内非分歧$\Longleftrightarrow \mathfrak{p}$在$L$内非分歧。

3. 设D为Dedekind整环，K为其比域，$F/K, E/K$为有限可离扩张(E，F含于K的同一代数闭包当中)。R为D在E中的整数闭包，$\mathfrak{p}$为D的一素理想，$\mathfrak{q}$为R的素理想，$\mathfrak{q} \cap D=\mathfrak{p}$，且$D/\mathfrak{p}$为完全域。证明：

(1) 如果$\mathfrak{p}$在F中完全分裂，则$\mathfrak{q}$在EF中完全分裂；

(2) 如果$\mathfrak{p}$在F中非分歧，则$\mathfrak{q}$在EF中非分歧。

4. 设D为Dedekind整环，K为其比域，L/K为有限伽罗瓦扩张，S为D在L中的整数闭包，$\mathfrak{q}$为S中非零素理想，$\mathfrak{p}=\mathfrak{q} \cap D$，$\mathfrak{q}$的分解群和惯性群分别记为$G_Z$和$G_T$。证明：

(1) $G_Z \cong G(\hat{L}/\hat{K})$；

(2) G_T同构于$\mathfrak{q}\hat{S}$对$\hat{L}/\hat{K}$的惯性群，

其中$\hat{L}, \hat{S}$和$\hat{K}$分别表示L，S(对$\mathfrak{q}$-adic拓扑)和K(对$\mathfrak{p}$-adic拓扑)的完备化。

5. 设K为数域，L/K为伽罗瓦扩张，D和S分别表示K和L中的代数整数环，$\mathfrak{q}$为S中的非零素理想。定义

$$\Gamma_i=\{\sigma \in G(L/K): \sigma(x) \equiv x (\bmod \mathfrak{q}^{i+1}), \forall x \in S\}$$

$(i=1,2,\cdots)$，称 Γ_i 为 $\mathfrak{q}$ 的第 i 个分歧群。证明：

(1) $G_T \supset \Gamma_1 \supset \Gamma_2 \supset \cdots$；

(2) G_T/Γ_1 与域 $S/\mathfrak{q}$ 的非零元素乘法群的某子群同构，故 G_T/Γ_1 为循环群；

(3) $\Gamma_i/\Gamma_{i+1} (i=1,2,\cdots)$ 与 $S/\mathfrak{q}$ 加法群的子群同构，故为交换 p 群。

(4) $\mathfrak{q}$ 的分解群 G_Z 是可解群。

6. 设 $\zeta=\exp(2\pi i/m)$，其中 m 为奇数或 $4|m$。令 $\mathbf{Q}(\zeta)$ 的代数整数环为 R。设 p 为素数，$\mathfrak{p}$ 为 R 的一个素理想，$\mathfrak{p}\cap \mathbf{Z}=p\mathbf{Z}$。证明：

(1) $[\mathbf{Q}(\zeta):\mathbf{Q}]=\varphi(m)$，$\varphi$ 为尤拉函数；

(2) 若 $p\nmid m$，则 $\zeta^i \equiv \zeta^j \pmod{\mathfrak{p}} \Longleftrightarrow i\equiv j \pmod{m}$；

(3) 若 $p\nmid m$，则

$$pR=\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_g,$$

其中 $\mathfrak{p}_i$ 为 R 中的素理想，$\mathfrak{p}_i$ 对 $p\mathbf{Z}$ 的剩余次数是使得

$$p^f\equiv 1 \pmod{m}$$

成立的最小正整数 f，$g=\varphi(m)/f$；

(4) 若 $p|m$，令 $m=p^r m'$，$(m',p)=1$，则

$$pR=(\mathfrak{p}_1\cdots\mathfrak{p}_g)^{\varphi(p^r)},$$

其中 $\mathfrak{p}_i$ 为 R 中的素理想，$\mathfrak{p}_i$ 对 $p\mathbf{Z}$ 的剩余次数是使得

$$p^f\equiv 1 \pmod{m'}$$

的最小正整数 f，$g=\varphi(m')/f$。

第九章 同调代数

§1 复合形

同调代数起源于拓扑学。我们考虑如下的情形：取一个三角形（图9.1）。令有向三角形ABC为a，有向线段AB，BC，CA为b_1,b_2,b_3，三点A，B，C为c_1,c_2,c_3。又令d为**边缘算子**。我们立得

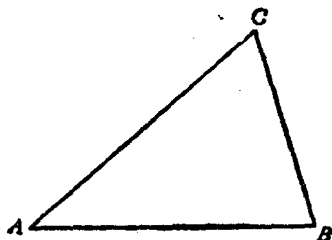


图 9.1

$$d(a)=b_1+b_2+b_3,$$
$$d(b_1)=c_2-c_1,\quad d(b_2)=c_3-c_2,\quad d(b_3)=c_1-c_3,$$
$$d(c_i)=0,\quad i=1,2,3.$$

容易验证

$$d^2(a)=d(d(a))=0,\quad d^2(b_i)=0,\quad i=1,2,3.$$

我们可以引入代数结构：令C_2为a生成的自由交换群，C_1为b_1，b_2,b_3生成的自由交换群，C_0为c_1,c_2,c_3生成的自由交换群。我们自然扩充d为$C_2\to C_1$，$C_1\to C_0$，$C_0\to 0$的群映射，得出下图：

$$C_2\xrightarrow{d}C_1\xrightarrow{d}C_0\xrightarrow{d}0.$$

为了清楚起见，我们把上面的d用三种符号表示如下：

$$C_2\xrightarrow{d_2}C_1\xrightarrow{d_1}C_0\xrightarrow{d_0}0.$$

显然，d_i适合

$$d_{i-1}d_i=0,\quad i=1,2.$$

我们注意到"交换群"是一种"$\boldsymbol{Z}$模"，因此，可以推广上面的讨

论到一般的环R的模上去。

定义9.1 设R为一环。所谓一个R**复合形**(C,d)，即是一组R模C_i $(i\in \boldsymbol{Z})$ 及R映射d_i: $C_i\to C_{i-1}$，适合$d_{i-1}d_i=0$。又设(C,d),(C',d')为两个R复合形，所谓(C,d)到(C',d')的映射a是指一组映射a_i: $C_i\to C'_i$，使

$$a_{i-1}d_i=d'_i a_i,$$

或写成

$$ad=da.$$

也即是说，下图

$$\begin{array}{ccc} C_i & \xrightarrow{d_i} & C_{i-1} \\ {\scriptstyle a_i}\downarrow & & \downarrow{\scriptstyle a_{i-1}} \\ C'_i & \xrightarrow{d'_i} & C'_{i-1} \end{array}$$

是可交换的。

例1 在上面讨论的拓扑学的例子中，我们可以令

$$C_3=C_4=\cdots=0,\qquad C_{-1}=C_{-2}=\cdots=0,$$
$$d_3=d_4=\cdots=0,\qquad d_{-1}=d_{-2}=\cdots=0.$$

则(C,d)成为一个适合定义9.1的$\boldsymbol{Z}$复合形。

例2 设$K=\mathbf{C}[x,y,z]$,

$$C_0=K,\qquad C_{-1}=Kdx\oplus Kdy\oplus Kdz,$$
$$C_{-2}=K(dy\wedge dz)\oplus K(dz\wedge dx)\oplus K(dx\wedge dy),$$
$$C_{-3}=K(dx\wedge dy\wedge dz),$$

此处“$\wedge$”是外积，即

$$dx\wedge dx=dy\wedge dy=dz\wedge dz=0,$$

$$dx\wedge dy=-dy\wedge dx,\quad dy\wedge dz=-dz\wedge dy,\quad dz\wedge dx=-dx\wedge dz.$$

我们定义

$$d_0(f(x,y,z))=\frac{\partial f}{\partial x}dx+\frac{\partial f}{\partial y}dy+\frac{\partial f}{\partial z}dz,$$

$$d_{-1}(f_1dx+f_2dy+f_3dz)$$

$$=\left(\frac{\partial f_3}{\partial y}-\frac{\partial f_2}{\partial z}\right)dy\wedge dz+\left(\frac{\partial f_1}{\partial z}-\frac{\partial f_3}{\partial x}\right)dz\wedge dx$$

$$+\left(\frac{\partial f_2}{\partial x}-\frac{\partial f_1}{\partial y}\right)dx\wedge dy$$

$$d_{-2}(f_1dy\wedge dz+f_2dz\wedge dx+f_3dx\wedge dy)$$

$$=\left(\frac{\partial f_1}{\partial x}+\frac{\partial f_2}{\partial y}+\frac{\partial f_3}{\partial z}\right)dx\wedge dy\wedge dz.$$

请注意：d_0 即是高等微积分中的梯度算子，d_{-1} 即旋度算子，d_{-2} 即散度算子。我们定义其余的 C_i 及 d_i 皆为 0。如此则定义出一个**C** 复合形。▎

设(C, d)是一个R复合形。从下式

$$d_id_{i+1}C_{i+1}=0$$

立得 d_{i+1} 的象 $d_{i+1}C_{i+1}$ 包含在 d_i 的核之中。我们常用 Z_i 表示 d_i 的核，其中的元素称为 i **阶闭链**，或简称为**闭链**；又用 B_i 表示 $d_{i+1}C_{i+1}$，其中的元素称为 i **阶边缘**，或简称为**边缘**。于是有 $B_i\subset Z_i$，二者皆是R模。

定义9.2 商模 Z_i/B_i 称为R复合形(C,d)的 i **阶同调模**，记为 $H_i=H_i(C)$。

例 3 计算上面两个例子的同调模。在例 1 中，

$$Z_0=\boldsymbol{Z}c_1\oplus\boldsymbol{Z}c_2\oplus\boldsymbol{Z}c_3,$$

$$B_0=\boldsymbol{Z}(c_2-c_1)+\boldsymbol{Z}(c_3-c_2)+\boldsymbol{Z}(c_1-c_3),$$

所以
$$H_0=Z_0/B_0\approx\boldsymbol{Z}.$$

又
$$Z_1=\boldsymbol{Z}(b_1+b_2+b_3)=B_1,$$

所以
$$H_1=Z_1/B_1=0.$$

又
$$Z_2=0=B_2,$$

所以
$$H_2=Z_2/B_2=0.$$

其余的 H_i 皆为0。

现在计算例 2。显然有

$$d_0(f(x,y,z))=0 \iff f(x,y,z)\in \mathbf{C},$$

立得 $H_0=Z_0/B_0=\mathbf{C}/(0)\approx\mathbf{C}$。又有

$$d_{-1}(f_1dx+f_2dy+f_3dz)=0$$

$$\iff \frac{\partial f_3}{\partial y}=\frac{\partial f_2}{\partial z},\quad \frac{\partial f_1}{\partial z}=\frac{\partial f_3}{\partial x},\quad \frac{\partial f_2}{\partial x}=\frac{\partial f_1}{\partial y}$$

$\iff$存在$g(x,y,z)$，使得

$$d_0(g(x,y,z))=f_1dx+f_2dy+f_3dz$$

（高等微积分定理）

$$\iff f_1dx+f_2dy+f_3dz\in B_1,$$

所以 $H_{-1}=Z_{-1}/B_{-1}=0$。又有

$$d_{-2}(f_1dy\wedge dz+f_2dz\wedge dx+f_3dx\wedge dy)=0$$

$$\iff \frac{\partial f_1}{\partial x}=\frac{\partial f_2}{\partial y}=\frac{\partial f_3}{\partial z}=0$$

$\iff$存在$h_1dx+h_2dy+h_3dz$，使得

$$d_{-1}(h_1dx+h_2dy+h_3dz)$$
$$=f_1dy\wedge dz+f_2dz\wedge dx+f_3dx\wedge dy$$

（高等微积分定理）

$$\iff f_1dy\wedge dz+f_2dz\wedge dx+f_3dx\wedge dy\in B_{-2},$$

所以
$$H_{-2}=Z_{-2}/B_{-2}=0。$$

又不难看出

$$Z_{-3}=K(dx\wedge dy\wedge dz),$$

及任取 $g(x,y,z)dx\wedge dy\wedge dz$，总可以找到 $f(x,y,z)$，使得

$$\frac{\partial f}{\partial x}=g(x,y,z),$$

也即

$$d_{-2}(fdy\wedge dz)=g(x,y,z)dx\wedge dy\wedge dz,$$

所以
$$H_{-3}=Z_{-3}/B_{-3}=0。$$

其余的H_i皆为0。

请问读者，本例中两次提到的高等微积分中的定理，是指什么？请向梯度、旋度、散度三算子的方向去追查。

例4 令 $K=\mathbf{C}((x))$，即所有的形式的亚纯函数构成的域。令 $C_0=K$，$C_{-1}=Kdx$；d_0的定义如下：

$$d_0 f(x)=f'(x)dx.$$

我们定义其余的C_i及d_i皆为0。则(C,d)显然是$\mathbf{C}$复合形。现在我们来计算H_i。首先，

$$Z_0=\mathbf{C},\qquad B_0=0,$$

所以
$$H_0=Z_0/B_0\approx\mathbf{C}.$$

不难看出，$Z_{-1}=C_{-1}=Kdx$。任取 $g(x)\in K$，

$$g(x)=\sum_{i=-m}^{\infty}a_i x^i,$$

则，存在 $f(x)\in K$，使 $f'(x)=g(x)\Longleftrightarrow a_{-1}=0$。所以

$$B_{-1}=\left\{\sum_i a_i x^i dx:\ a_{-1}=0\right\}.$$

于是，映射

$$r:\ H_{-1}=Z_{-1}/B_{-1}\to\mathbf{C},$$

$$r\left(\sum_i a_i x^i\,dx\right)=a_{-1}$$

是同构。所以$H_{-1}\approx\mathbf{C}$。这里的r即是复变函数论中的“剩余映射”。与前面的例子相同，其余的H_i皆为0。▌

如果对所有的$i<0$，C_i皆为0，我们常称此种复合形为**正复合形**或**链复合形**；反之，如果对所有的$i>0$，C_i皆为0，则称此种复合形为**负复合形**或**上链复合形**。在上链复合形中，通常改变符号，记

$$C^i=C_{-i},\qquad d^i=d_{-i},$$

于是有

$$0 \longrightarrow C^0 \xrightarrow{d^0} C^1 \xrightarrow{d^1} C^2 \xrightarrow{d^2} \cdots.$$

所有的术语也仿此改称为**上闭链**、**上边缘**、**上同调模**等等.

当 $H_i(C)=0$ 时，我们自然得出

$$Z_i = B_i, \qquad \ker d_i = \operatorname{im} d_{i+1}.$$

此时我们称复合形在 i 处是"正合的"。一般言之，我们有

定义9.3 设A, B, C是R模. 在下列图形中,

$$A \xrightarrow{\alpha} B \xrightarrow{\beta} C,$$

此处 α, β 是模映射，如果有

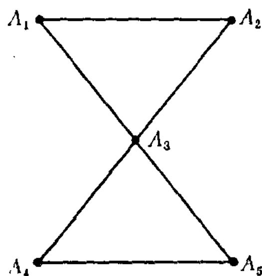
$$\operatorname{im} \alpha = \ker \beta,$$

则称上面的序列在B处是**正合的**，或在中央处是正合的.

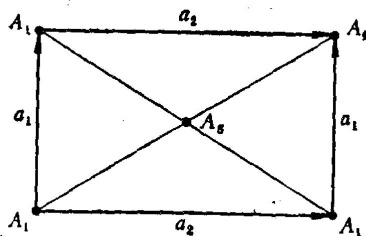
习　题

1． 计算8字形的同调模。复合形如图。

2． 计算圆环面的同调模，复合形如图。（把正方形两边对粘起来，成为一个筒形，再把筒形的两圆边粘起来，则成一圆环面。）



题1图



题2图

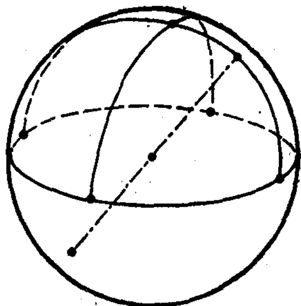
3． 计算实射影平面(real projective plane)的同调模：复合形如图。（实射影平面即粘合二维球面的对径点所得出的拓扑空

间。）

4． 本节例3中所提到的"高等微积分"中的定理是什么？

5． 参考例2及例3，令

$K = \{$三维空间 $\boldsymbol{R}^3$ 上的可微函数$\}$.



题3图

定义

$C_0 = K,$

$C_{-1} = Kdx \oplus Kdy \oplus Kdz,$

$C_{-2} = Kdy \wedge dz \oplus Kdz \wedge dx \oplus Kdx \wedge dy, \quad C_{-3} = Kdx \wedge dy \wedge dz.$

定义d_0, d_{-1}, d_{-2}如例2。证明 $H_0(C) \approx \boldsymbol{R}$，其余 $H_i(C) = 0$。

6． 仿照例4，用 $\boldsymbol{C}\{\{x\}\} = \{$在0点附近的亚纯函数$\}$ 代替 $\boldsymbol{C}((x))$，构造复合形C，再计算 $H_i(C)$。请注意 $\boldsymbol{C}\{\{x\}\}$ 的元素在0点的一个邻域$N\backslash\{0\}$是解析函数。

7． 设K是域，(C,d)是一个K模复合形。假设

$$\sum \dim C_i < +\infty.$$

证明

$$\sum(-1)^i \dim C_i = \sum(-1)^i \dim H_i(C).$$

8． 设M是一个R模，令 $C_i = M (i \in \boldsymbol{Z})$，及 $d_i = 0$。证明这样得到一个R模复合形，并求$H_i(C)$。

9． 给定R模正合序列

$$0 \longrightarrow M_1 \xrightarrow{\alpha} M \xrightarrow{\beta} M_2 \longrightarrow 0,$$

我们令 $C_i = 0 (i \leqslant 0)$，$C_1 = M_2$，$C_2 = M, C_3 = M_1, C_j = 0 (j \geqslant 4)$。又令 $d_2 = \beta$，$d_3 = \alpha$，$d_j = 0 (j \neq 2, 3)$。证明这样得到一个R模复合形，并求$H_i(C)$。

10． 设G是有限交换群，$R = \boldsymbol{Z}[G]$为整系数群环。作G的笛卡尔乘积：

$$G^{i+1} = \overbrace{G \times G \times \cdots \times G}^{i+1} \quad (i \geqslant 0),$$

令 C_i 是由 G^{i+1} 生成的自由交换群，而 $C_j=0$ $(j<0)$. 对任意 $g\in G$，定义它在 C_i 的基元素的作用为

$$g(g_0,g_1,\cdots,g_i)=(gg_0,gg_1,\cdots,gg_i).$$

按线性原则扩充为 R 在 C_i 上的作用，使 C_i 成为 R 模. 定义 d_i 在 C_i 的基元素上的作用为

$$d_i(g_0,\cdots,g_i)=\sum_{j=0}^{i}(-1)^j(g_0,\cdots,g_{j-1},g_{j+1},\cdots,g_i)\quad(i\geqslant 0),$$

$$d_i=0\quad(i<0).$$

再按线性原则扩充为 C_i 到 C_{i-1} 的 R 模映射. 证明这样得出一个 R 模复合形.

11. 设 α 是 R 模复合形 (C,d) 到 R 模复合形 (C',d') 的映射，使下图

$$\begin{array}{ccccccc}\cdots\longrightarrow & C_i & \xrightarrow{d_i} & C_{i-1} & \longrightarrow\cdots\\ & \downarrow{\scriptstyle\alpha_i} & & \downarrow{\scriptstyle\alpha_{i-1}} & \\ \cdots\longrightarrow & C'_i & \xrightarrow{d'_i} & C'_{i-1} & \longrightarrow\cdots\end{array}$$

交换. 令 $C''_i=C_{i-1}\oplus C'_i\,(i\in \boldsymbol{Z})$，对 $x_{i-1}\in C_{i-1}$ 和 $x'_i\in C'_i$，定义

$$d''_i(x_{i-1},x'_i)=(-d_{i-1}x_{i-1},\alpha_{i-1}x_{i-1}+d'_ix'_i).$$

证明 (C'',d'') 是一个 R 模复合形.

12. 设 (C,d) 是 $\boldsymbol{Z}$ 模复合形，其中每个 C_i 都是自由 $\boldsymbol{Z}$ 模，证明 Z_n 和 B_n 也是自由 $\boldsymbol{Z}$ 模，且 Z_n 是 C_n 的直和因子.

§2 同调序列

设 (C,d) 及 (C'',d'') 为两个复合形，$\beta=\{\beta_i\}: C\to C''$ 为映射. 在下列图形中，

$$\begin{array}{ccccccc}\longrightarrow & C_{i+1} & \xrightarrow{d_{i+1}} & C_i & \xrightarrow{d_i} & C_{i-1} & \longrightarrow\\ & \downarrow{\scriptstyle\beta_{i+1}} & & \downarrow{\scriptstyle\beta_i} & & \downarrow{\scriptstyle\beta_{i-1}} & \\ \longrightarrow & C''_{i+1} & \xrightarrow{d''_{i+1}} & C''_i & \xrightarrow{d''_i} & C''_{i-1} & \longrightarrow\end{array}$$

任取 $z_i \in Z_i$，$b_i \in B_i$，则有

$$0 = \beta_{i-1} d_i(z_i) = d''_i \beta_i(z_i),$$

所以$\beta_i(z_i) \in Z''_i$。令

$$b_i = d_{i+1}(a_{i+1}), \quad a_{i+1} \in C_{i+1},$$

则

$$\beta_i(b_i) = \beta_i d_{i+1}(a_{i+1}) = d''_{i+1}(\beta_{i+1}(a_{i+1})),$$

即 $\beta_i(b_i) \in B''_i$。所以可以定义

$$\bar{\beta}_i: H_i(C) \to H_i(C''),$$

$$\bar{\beta}_i([z_i]) = [\beta_i(z_i)].$$

这里$[z_i]$表示 z_i 在同调群 $H_i(C)$中代表的元素(同调类)。

例5 我们应用例1．令(C,d)为例1的 $\boldsymbol{Z}$ 复合形，(C',d')相应于三角形的边界，即

$$C'_1 = \boldsymbol{Z}b_1 \oplus \boldsymbol{Z}b_2 \oplus \boldsymbol{Z}b_3, \quad C'_0 = \boldsymbol{Z}c_1 \oplus \boldsymbol{Z}c_2 \oplus \boldsymbol{Z}c_3,$$

$$C'_i = 0, \quad \forall i \neq 0,1.$$

我们定义映射 $\alpha = \{\alpha_i\}: C' \to C$，其中 α_1, α_0 为等同映射，其余的 α_i 皆为 0．不难算出

$$Z'_1 = \boldsymbol{Z}(b_1 + b_2 + b_3), \quad B'_1 = 0,$$

$$H_1(C') \approx \boldsymbol{Z}, \quad H_0(C') \approx \boldsymbol{Z},$$

其余的 $H_i(C')$均为 0．此时 $\bar{\alpha}_0$为等同映射，$\bar{\alpha}_1$为 0 映射，其余的 $\bar{\alpha}_i$ 均为 0 映射。▌

参考上面的例子，设有R复合形(C,d)，(C',d')及映射$\alpha: C' \to C$，我们可以进一步地构成一个R复合形(C'',d'') 如下：令

$$C''_i = C_i/\alpha_i(C'_i);$$

又，当 $a''_i = \bar{a}_i \in C''_i$ 时，令

$$d''_i(a''_i) = \overline{d_i(a_i)}.$$

显而易见，当 $\bar{a}_i = \bar{f}_i$ 时，有 $a_i = f_i + \alpha(a'_i)$，$a'_i \in C'_i$。于是有

$$\overline{d_i(a_i)} = \overline{d_i(f_i) + d_i\alpha_i(a'_i)}$$

$$= \overline{d_i(f_i) + \alpha_{i-1}d'_i(a'_i)} = \overline{d_i(f_i)},$$

所以 d''_i 的定义是良好的。易于验证(C'',d'')为一个R复合形。

如此得出的三组同调模序列 $H_i(C), H_i(C'), H_i(C'')$ 之间有何关系？为此，我们引入定义：

定义9.4 设有复合形C', C, C''及映射

$$C' \xrightarrow{\alpha} C \xrightarrow{\beta} C''.$$

如果对任意的 i，序列

$$0 \longrightarrow C'_i \xrightarrow{\alpha_i} C_i \xrightarrow{\beta_i} C''_i \longrightarrow 0$$

都是正合的，即：α_i是单射，β_i是满射，$\operatorname{im} \alpha_i = \ker \beta_i$，则我们称 $C' \xrightarrow{\alpha} C \xrightarrow{\beta} C''$ **为短正合序列.**

定理9.1 设 $C' \xrightarrow{\alpha} C \xrightarrow{\beta} C''$是短正合序列，则存在一组连结映射 $\Delta_i (i \in \boldsymbol{Z})$，使下面的同调模序列为正合序列：

$$\cdots \longrightarrow H_i(C') \xrightarrow{\tilde{\alpha}_i} H_i(C) \xrightarrow{\tilde{\beta}_i} H_i(C'') \xrightarrow{\Delta_i} H_{i-1}(C') \xrightarrow{\tilde{\alpha}_{i-1}} \cdots.$$

证明 此定理的证法是所谓“查图法”. 这是同调代数的标准证明方法之一，读者应该细心体会. 我们作下图：

$$\begin{array}{ccccccccccc}
 & & 0 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
\cdots \longrightarrow & & C'_{i+1} & \xrightarrow{d'_{i+1}} & C'_i & \xrightarrow{d'_i} & C'_{i-1} & \xrightarrow{d'_{i-1}} & C'_{i-2} & \longrightarrow \cdots \\
 & & \downarrow{\scriptstyle \alpha_{i+1}} & & \downarrow{\scriptstyle \alpha_i} & & \downarrow{\scriptstyle \alpha_{i-1}} & & \downarrow{\scriptstyle \alpha_{i-2}} & & \\
\cdots \longrightarrow & & C_{i+1} & \xrightarrow{d_{i+1}} & C_i & \xrightarrow{d_i} & C_{i-1} & \xrightarrow{d_{i-1}} & C_{i-2} & \longrightarrow \cdots \\
 & & \downarrow{\scriptstyle \beta_{i+1}} & & \downarrow{\scriptstyle \beta_i} & & \downarrow{\scriptstyle \beta_{i-1}} & & \downarrow{\scriptstyle \beta_{i-2}} & & \\
\cdots \longrightarrow & & C''_{i+1} & \xrightarrow{d''_{i+1}} & C''_i & \xrightarrow{d''_i} & C''_{i-1} & \xrightarrow{d''_{i-1}} & C''_{i-2} & \longrightarrow \cdots \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & & 0 & &
\end{array}$$

取$z''_i \in Z''_i$. 因为 i 列是正合的，所以必有 $z_i \in C_i$，使

$$z''_i = \beta_i(z_i),$$

此处所取的z_i有几分任意性。我们有

$$\beta_{i-1}d_i(z_i)=d''_i\beta_i(z_i)=d''_i(z''_i)=0.$$

因为$i-1$列是正合的，即

$$\mathrm{im}\ \alpha_{i-1}=\ker\beta_{i-1}\ni d_i(z_i),$$

所以存在唯一的$z'_{i-1}\in C'_{i-1}$，使

$$\alpha_{i-1}(z'_{i-1})=d_i(z_i).$$

令$\Delta_i([z''_i])=[z'_{i-1}]$。自然有

$$\alpha_{i-2}d'_{i-1}(z'_{i-1})=d_{i-1}\alpha_{i-1}(z'_{i-1})=d_{i-1}d_i(z_i)=0,$$

因为α_{i-2}是单射，所以$d'_{i-1}(z'_{i-1})=0$，即$z'_{i-1}\in Z'_{i-1}$，$[z'_{i-1}]$确为$H_{i-1}(C')$中的元素。

如此规定的Δ_i是否是良好的？我们研究z_i的任意性。设另有一个$\bar{z}_i$，同样适合$z''_i=\beta_i(\bar{z}_i)$，则

$$\beta_i(z_i-\bar{z}_i)=z''_i-z''_i=0.$$

利用i列的正合性，立得

$$z_i-\bar{z}_i=\alpha_i(z'_i)\in\mathrm{im}\ \alpha_i=\ker\beta_i,\qquad z'_i\in C'_i.$$

令相当于z'_{i-1}的元素为$\bar{z}'_{i-1}$，即$\alpha_{i-1}(\bar{z}'_{i-1})=d_i(\bar{z}_i)$，则有

$$\alpha_{i-1}(z'_{i-1}-\bar{z}'_{i-1})=d_i(z_i-\bar{z}_i)=d_i\alpha_i(z'_i)=\alpha_{i-1}d'_i(z'_i).$$

因为α_{i-1}是单射，所以得出

$$z'_{i-1}-\bar{z}'_{i-1}=d'_i(z'_i)\in B'_{i-1}.$$

所以，当考虑商模$H_{i-1}(C')=Z'_{i-1}/B'_{i-1}$时，此种任意性立刻消失了。

以下我们分三个步骤来证明本定理考虑的同调模序列的正合性：1) $\mathrm{im}\ \tilde{\alpha}_i=\ker\tilde{\beta}_i$；2) $\mathrm{im}\ \tilde{\beta}_i=\ker\Delta_i$；3) $\mathrm{im}\ \Delta_i=\ker\tilde{\alpha}_{i-1}$。

1) 任取$[z'_i]\in H_i(C')$，$z'_i\in Z'_i$。则有

$$\tilde{\beta}_i\tilde{\alpha}_i([z'_i])=\tilde{\beta}_i([\alpha_i(z'_i)])=[\beta_i\alpha_i(z'_i)]=0,$$

也即$\mathrm{im}\ \tilde{\alpha}_i\subset\ker\tilde{\beta}_i$。反过来，任取$z_i\in Z_i$，使得$[z_i]\in\ker\tilde{\beta}_i$。则有$0=\tilde{\beta}_i([z_i])=[\beta_i(z_i)]$，即

$$\beta_i(z_i)\in B''_i=\mathrm{im}\ d''_{i+1}.$$

所以存在z''_{i+1}及z_{i+1}，使

$$\beta_i(z_i)=d''_{i+1}(z''_{i+1}), \qquad z''_{i+1}=\beta_{i+1}(z_{i+1}).$$

于是 $\beta_i(z_i)=d''_{i+1}\beta_{i+1}(z_{i+1})=\beta_i d_{i+1}(z_{i+1})$，所以

$$0=\beta_i(z_i-d_{i+1}(z_{i+1})),$$

也即 $$z_i-d_{i+1}(z_{i+1})\in\ker\beta_i=\operatorname{im}\alpha_i.$$

于是存在$z'_i\in C'_i$，使

$$z_i-d_{i+1}(z_{i+1})=\alpha_i(z'_i).$$

从上式立得

$$[z_i]=[z_i-d_{i+1}(z_{i+1})]=[\alpha_i(z'_i)]$$
$$=\tilde{\alpha}_i([z'_i])\in\operatorname{im}\tilde{\alpha}_i.$$

2) 任取$[z_i]\in H_i(C)$，$z_i\in Z_i$。则有

$$\Delta_i\tilde{\beta}_i([z_i])=[z'_{i-1}],$$

其中z'_{i-1}是由$\alpha_{i-1}(z'_{i-1})=d_i(z_i)$决定的。立得

$$\alpha_{i-1}(z'_{i-1})=d_i(z_i)=0.$$

而α_{i-1}是单射，所以$z'_{i-1}=0$，也即

$$\Delta_i\tilde{\beta}_i([z_i])=0, \qquad \operatorname{im}\tilde{\beta}_i\subset\ker\Delta_i.$$

现在我们任取 $z''_i\in Z''_i$，适合 $\Delta_i([z''_i])=0$。任取 $z_i\in C_i$，使

$$z''_i=\beta_i(z_i),$$

则 $$\beta_{i-1}(d_i(z_i))=d''_i(\beta_i(z_i))=d''_i(z''_i)=0.$$

于是存在 $z'_{i-1}\in C'_{i-1}$，使$\alpha_{i-1}(z'_{i-1})=d_i(z_i)$。则有

$$0=\Delta_i([z''_i])=[z'_{i-1}].$$

于是

$$z'_{i-1}\in B'_{i-1}=\operatorname{im}d'_i,$$

也即存在 $z'_i\in C'_i$，使 $z'_{i-1}=d'_i(z'_i)$。代入上式，得

$$d_i(z_i)=\alpha_{i-1}(z'_{i-1})=\alpha_{i-1}d'_i(z'_i)=d_i\alpha_i(z'_i),$$

所以 $$d_i(z_i-\alpha_i(z'_i))=0.$$

我们同时有

$$\beta_i(z_i-\alpha_i(z'_i))=\beta_i(z_i)-\beta_i\alpha_i(z'_i)=\beta_i(z_i)=z''_i.$$

因此，我们令$\bar{z}_i=z_i-\alpha_i(z'_i)\in Z_i$，则有

$$\tilde{\beta}_i([\bar{z}_i])=[\beta_i(\bar{z}_i)]=[z''_i],$$

即$[z''_i]\in \operatorname{im}\tilde{\beta}_i$。

3) 任取$z''_i\in Z''_i$，$[z''_i]\in H_i(C'')$。令z_i, z'_{i-1}适合下式

$$z''_i=\beta_i(z_i),\qquad d_i(z_i)=a_{i-1}(z'_{i-1}),$$

则
$$\Delta_i([z''_i])=[z'_{i-1}].$$

立得
$$\tilde{a}_{i-1}\Delta_i([z''_i])=[a_{i-1}(z'_{i-1})]=[d_i(z_i)]=0.$$

于是

$$\operatorname{im}\Delta_i\subset\ker\tilde{a}_{i-1}.$$

现在我们任取$[z'_{i-1}]\in\ker\tilde{a}_{i-1}$，则

$$0=\tilde{a}_{i-1}([z'_{i-1}])=[a_{i-1}(z'_{i-1})],$$

即
$$a_{i-1}(z'_{i-1})\in B_{i-1},$$

也即存在$z_i\in C_i$，使

$$d_i(z_i)=a_{i-1}(z'_{i-1}).$$

令$z''_i=\beta_i(z_i)$，则有

$$d''_i(z''_i)=d''_i\beta_i(z_i)=\beta_{i-1}d_i(z_i)=\beta_{i-1}a_{i-1}(z'_{i-1})=0,$$

即

$$z''_i\in Z''_i.$$

根据Δ_i的定义，我们有

$$\Delta_i([z''_i])=[z'_{i-1}].\quad\blacksquare$$

例6 考虑例5，令(C'',d'')为下面的$\boldsymbol{Z}$复合形：

$$C''_2=C_2/a(C'_2)\approx C_2,$$
$$C''_1=C_1/a(C'_1)=0,$$
$$C''_0=C_0/a(C'_0)=0,$$

其余的C''_i皆为0。又令$\beta_i: C_i\to C''_i$为典型映射，则显然有一短正合列

$$0\longrightarrow C'\xrightarrow{a}C\xrightarrow{\beta}C''\longrightarrow 0.$$

于是，按照本定理，有下面的长正合列：

$$\cdots \longrightarrow H_3(C'') \xrightarrow{\Delta_3} H_2(C') \xrightarrow{\tilde{\alpha}_2} H_2(C) \xrightarrow{\tilde{\beta}_2} H_2(C'')$$

$$\xrightarrow{\Delta_2} H_1(C') \xrightarrow{\tilde{\alpha}_1} H_1(C) \xrightarrow{\tilde{\beta}_1} H_1(C'') \xrightarrow{\Delta_1} H_0(C')$$

$$\xrightarrow{\tilde{\alpha}_0} H_0(C) \xrightarrow{\tilde{\beta}_0} H_0(C'') \xrightarrow{\Delta_{-1}} H_{-1}(C') \longrightarrow \cdots.$$

经过实际计算后，代入H_i的值，则得出

$$\cdots \longrightarrow 0 \xrightarrow{\Delta_3} 0 \xrightarrow{\tilde{\alpha}_2} 0 \xrightarrow{\tilde{\beta}_2} \boldsymbol{Z} \xrightarrow{\Delta_2} \boldsymbol{Z} \xrightarrow{\tilde{\alpha}_1} 0$$

$$\xrightarrow{\tilde{\beta}_1} 0 \xrightarrow{\Delta_1} \boldsymbol{Z} \xrightarrow{\tilde{\alpha}_0} \boldsymbol{Z} \xrightarrow{\tilde{\beta}_0} 0 \xrightarrow{\Delta_{-1}} 0 \longrightarrow \cdots.$$

在拓扑学看来，$H_i(C'')$可以理解成**相对同调群**。▌

在同调代数中，有一个起源于拓扑学的概念：同伦。

定义9.5 设α，β是两个从复合形(C',d')到(C,d)的映射。如果存在一组模映射$s=\{s_i\}$，s_i: $C'_i\to C_{i+1}$，使得

$$\alpha_i-\beta_i=d_{i+1}s_i+s_{i-1}d'_i, \qquad \forall i,$$

则称α，β **同伦**，以符号$\alpha\sim\beta$表示之。

对上面的定义，我们可以图解如下。

$$\begin{array}{ccccccccc}
\cdots \longrightarrow & C'_{i+1} & \xrightarrow{d'_{i+1}} & C'_i & \xrightarrow{d'_i} & C'_{i-1} & \longrightarrow \cdots \\
& \Downarrow & \swarrow s_i & \alpha_i \Downarrow \beta_i & \swarrow s_{i-1} & \Downarrow & \\
\cdots \longrightarrow & C_{i+1} & \xrightarrow{d_{i+1}} & C_i & \xrightarrow{d_i} & C_{i-1} & \longrightarrow \cdots
\end{array}$$

同伦的意义在于下面的定理：

定理9.2 设α，β同伦，即$\alpha\sim\beta$，则

$$\tilde{\alpha}_i=\tilde{\beta}_i: H_i(C')\to H_i(C).$$

证明 任取$z'_i\in Z'_i$，则有

$$\bar{\alpha}_i([z'_i]) = [\alpha_i(z'_i)] = [(\beta_i + d_{i+1}s_i + s_{i-1}d'_i)(z'_i)]$$
$$= [(\beta_i + d_{i+1}s_i)(z'_i)] = [\beta_i(z'_i)]$$
$$= \bar{\beta}_i([z'_i]). \quad \blacksquare$$

例7 我们应用例5的讨论，令$\beta = \{\beta_i\}$定义如下：

$$\beta_i = 0, \quad i \neq 0,$$
$$\beta_0(n_1c_1 + n_2c_2 + n_3c_3) = (n_1 + n_2 + n_3)c_1.$$

显然，β是C'到C的映射。我们定义一组模映射$s = \{s_i\}$如下：

$$s_i = 0, \qquad i \neq 0, 1,$$

$$s_0(c_i) = \begin{cases} 0, & i = 1, \\ -b_1, & i = 2, \\ b_0, & i = 3. \end{cases}$$

$$s_1(b_i) = \begin{cases} 0, & i = 1, \\ a, & i = 2, \\ 0, & i = 3. \end{cases}$$

不难验证

$$\alpha_i - \beta_i = d_{i+1}s_i + s_{i-1}d'_i,$$

也即$\alpha \sim \beta$，所以$\bar{\alpha}_i = \bar{\beta}_i$。从拓扑学的观点来看，$\alpha$相当于三角形的等同映射，$\beta$相当于把三角形映射到一个顶点$c_1$，在允许考虑三角形内部的情形下，这两个映射是同伦的。

习　题

1. 设有R模映射交换图：

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \xrightarrow{u} & M & \xrightarrow{v} & M'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f''} & & \\ 0 & \longrightarrow & N' & \xrightarrow{u'} & N & \xrightarrow{v'} & N'' & \longrightarrow & 0 \end{array}$$

其中上、下两行正合。证明存在$\ker(f'')$到$N'/\mathrm{im}(f')$的模映射d，使下面序列正合：

$$0 \longrightarrow \ker(f') \xrightarrow{\tilde{u}} \ker(f) \xrightarrow{\tilde{v}} \ker(f'') \xrightarrow{d} N'/\mathrm{im}(f')$$

$$\xrightarrow{\tilde{u}'} N/\mathrm{im}(f) \xrightarrow{\tilde{v}'} N''/\mathrm{im}(f'') \longrightarrow 0,$$

其中$\tilde{u},\tilde{v},\tilde{u}',\tilde{v}'$分别由$u,v,u',v'$诱导而得。

2. 给定R模映射交换图如下.

$$\begin{array}{ccccc}
0 & \longrightarrow & 0 & \longrightarrow & 0 \\
\downarrow & & \downarrow & & \downarrow \\
K' & \xrightarrow{\delta'} & K & \xrightarrow{\delta} & K'' \\
\downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f''} \\
M' & \xrightarrow{\mu'} & M & \xrightarrow{\mu} & M'' \\
\downarrow{\scriptstyle g'} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle g''} \\
N' & \xrightarrow{\nu'} & N & \xrightarrow{\nu} & N'' \\
\downarrow{\scriptstyle h'} & & \downarrow{\scriptstyle h} & & \downarrow{\scriptstyle h''} \\
C' & \xrightarrow{\gamma'} & C & \xrightarrow{\gamma} & C'' \\
\downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & 0 & \longrightarrow & 0
\end{array}$$

在图中每个列和中间两行是正合的。令$x''\in K''$, $y\in M$, 满足$\mu y=f''x''$。那么$\nu gy=g''\mu y=g''f''x''=0$,且存在唯一的$z'\in N'$. 使得$\nu'z'=gy$。定义$\Delta x''=h'z'$。证明$\Delta x''$与$y$的选择无关，且$\Delta$: $K''\to C'$是一个模映射。验证

$$K' \xrightarrow{\delta'} K \xrightarrow{\delta} K'' \xrightarrow{\Delta} C' \xrightarrow{\gamma'} C \xrightarrow{\gamma} C''$$

是正合的。证明若μ'是单射，那么δ'也是单射。若ν是满射，那么γ也是满射。

3. 设R模复合形(C,d)到(C',d')的两个映射α,β是同伦的：$\alpha\sim\beta$，又设R模复合形(C',d')到(C'',d'')的两个映射γ, δ也同伦：$\gamma\sim\delta$。试证明R模复合形(C,d)到(C'',d'')的两个映

射 $\gamma\alpha,\delta\beta$ 必同伦：$\gamma\alpha\sim\delta\beta$。

4． 证明"3×3引理"：在下列复合形图中

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & A_1 & \longrightarrow & A_2 & \longrightarrow & A_3 & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & B_1 & \longrightarrow & B_2 & \longrightarrow & B_3 & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & C_1 & \longrightarrow & C_2 & \longrightarrow & C_3 & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

假设在三行与三列中，除了一行(或一列)以外，其它都正合，证明该行(或该列)必定也是正合的。

提示：读者可以利用每一行都是复合形，再利用定理9.1。

5． 考虑 $\boldsymbol{Z}$ 模复合形 (C,d)，(C',d')，其中

$$C_1=(s_1)\approx\boldsymbol{Z},\quad C_0=(s_0)\approx\boldsymbol{Z},\quad C_n=0\ \ (n\neq0,1);$$

$$d_1(s_1)=2s_0,\quad d_i=0\ \ (i\neq1);$$

$$C_1'=(t_1)\approx\boldsymbol{Z},\quad C_n'=0\ \ (n\neq1).$$

定义 (C,d) 到 (C',d') 的映射 φ 如下：

$$\varphi_1(s_1)=t_1,\quad \varphi_i=0\ \ (i\neq1).$$

证明 φ 与 (C,d) 到 (C',d') 的零映射不同伦。

6． 举例说明：如果 R 模复合形 (C,d) 到 (C',d') 的两个映射 α,β 诱导出它们的同调模 $H_i(C)$ 与 $H_i(C')$ 之间的同一个模映射，α 与 β 可能并不同伦。

§3 模的化解

模论与向量空间论的不同点之一是一般的模并非自由模。我

们可以用下面的方法来研究一般的模。

定义9.6 令M为R模。对于正复合形(C,d):

$$\cdots \longrightarrow C_n \xrightarrow{d_n} C_{n-1} \longrightarrow \cdots \longrightarrow C_1 \xrightarrow{d_1} C_0 \longrightarrow 0,$$

如果存在一个模映射 $\varepsilon: C_0 \to M$, 使$\varepsilon d_1 = 0$, 则称(C,d)为M**上的复合形**, ε为**投入映射**. 更进一步, 如果下面的序列是正合的, 则称C是M的**化解序列**:

$$\cdots \longrightarrow C_n \xrightarrow{d_n} C_{n-1} \longrightarrow \cdots \longrightarrow C_1 \xrightarrow{d_1} C_0 \xrightarrow{\varepsilon} M \longrightarrow 0.$$

讨论 1) 如果C是M的化解序列, 则显然有

$$H_i(C) = 0, \qquad \forall i > 0,$$

$$H_0(C) = C_0/d_1(C_1) = C_0/\ker\ \varepsilon \approx M.$$

2) 如果C_i又皆是自由模, 则称C是M的**自由化解序列**. 任给M, 可以用下面的方法建造M的一个自由化解序列; 令$\{m_i\}$是M的一个生成元集, 取符号x_i, 令$C_0 = \bigoplus_i Rx_i$, 定义

$$\varepsilon\left(\sum_i r_i x_i\right) = \sum_i r_i m_i.$$

设$K_0 = \ker \varepsilon$. 令$\{k_i^0\}$是K_0的一个生成元集. 取符号$\{x_i^0\}$, 令$C_1 = \bigoplus_i Rx_i^0$, 定义

$$d_1\left(\sum_i r_i x_i^0\right) = \sum_i r_i k_i^0.$$

再设$K_1 = \ker d_1$. 以此顺序建造$C_2, d_2, C_3, d_3, \cdots$, 即得$M$的自由化解序列$C = (C,d)$.

例8 设$R = \mathbf{C}[x,y]$, $M = (f(x,y))$, $N = (g(x,y), h(x,y))$, 其中$g(x,y)$, $h(x,y)$无公因子. 则M, N有下列的自由化解序列:

$$0 \longrightarrow R \xrightarrow{\varepsilon_1} M \longrightarrow 0,$$

$$0 \longrightarrow R \xrightarrow{d_1} R \oplus R \xrightarrow{\varepsilon_2} N \longrightarrow 0,$$

此处

$$\varepsilon_1(1) = f(x,y),$$

$$\varepsilon_2((1,0)) = g(x,y), \quad \varepsilon_2((0,1)) = h(x,y),$$
$$d_1(1) = (h(x,y), -g(x,y)).$$

讨论 不难看出，任给R及一自由模M，则存在一个自由化解序列

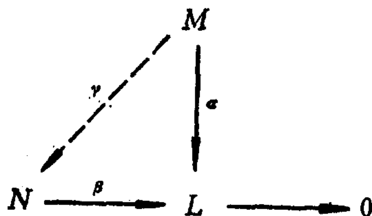
$$0 \longrightarrow M \longrightarrow M \longrightarrow 0.$$

所以我们可以用模N的最短自由化解序列的长度来度量N与自由模的偏差。上面的例子中，模M是自由模；模N虽非自由模，可是“偏差度”是1。

更进一步说，如果环R是域，则任意R模都是自由模。所以对任意环R，我们研究所有的R模与自由模的偏差，这可以当成环R与域的偏差性的度量。▍

比自由模广义且一样好用的是“射影模”。我们定义如下。

定义9.7 如果对任意的模映射$\alpha: M \to L$及任意的模满射$\beta: N \to L$，必有模映射$\gamma: M \to N$，使$\alpha = \beta\gamma$，则称模M是**射影模**。换言之，在下面的图形中



虚线部分可用γ补足，使此图形为可交换的。

讨论 1）任意的自由模都是射影模。事实上，设M是自由模，

$$M = \bigoplus_i Rm_i.$$

令$n_i \in N$，适合

$$\alpha(m_i) = \beta(n_i), \quad \forall i,$$

又令$\gamma: M \to N$，定义如下

$$\gamma(m_i) = n_i, \quad \forall i,$$

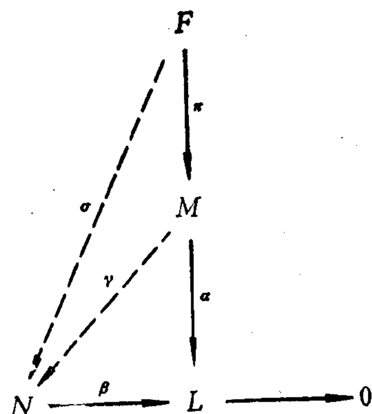
则显然有

$$\alpha=\beta\gamma.$$

2）一个模 M 是射影模的充要条件是：它是一个自由模 F 的**直和因子**。换言之，即存在一个模 G，使

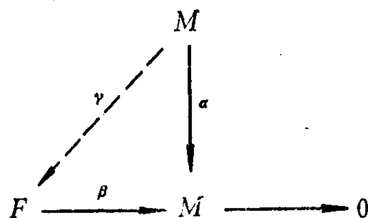
$$F=M\oplus G.$$

我们先讨论充分性，请见下图：



此处 $\pi(m,g)=m(m\in M,\ g\in G)$ 为 F 到 M 的投影映射。根据上面的讨论 1），存在 σ，使 $\alpha\pi=\beta\sigma$。令 $\gamma=\sigma|_M$(即 γ 为 σ 在 M 上的限制)即可。

现在我们讨论必要性。用定义 9.6 后面的讨论 2），令 F 为一个自由模(即 C_0)，则有下图：



此处 $\alpha=\mathrm{id}$ 是恒同映射。于是存在 γ，使

$$\alpha=\beta\gamma.$$

令 $G=\ker\beta$，则有 $G\cap\gamma(M)=\{0\}$，$F=G+\gamma(M)$。从这里我们立得 $F=G\oplus\gamma(M)$。又因为 γ 是单射，所以存在自由模$F^*\approx F$，使$F^*=G\oplus M$。

3）我们可以用同样的方法得出 M 是射影模的另一个充要条件如下：任给一个短正合序列

$$0\longrightarrow N\xrightarrow{\alpha}L\xrightarrow{\beta}M\longrightarrow 0,$$

必存在 $\gamma: M\to L$，使得 $\beta\gamma=1_M$（即M的恒同映射）.

4）应用上面的讨论，及中国剩余定理，令 $R=\boldsymbol{Z}/(mn)$，$(m,n)=1$，及$M=\boldsymbol{Z}/(m)$，$G=\boldsymbol{Z}/(n)$，则M,G都是R模，而且

$$R=G\oplus M.$$

所以 M 是射影模，且显然不是自由模(数一数，M中有多少个元素？)。由此可知，并非所有的射影模都是自由模。 ▎

我们引入如下的定义：

定义9.8 如果 C_i 都是射影模，则称复合形(C,d)为**射影复合形**；如果C是 M的化解序列，C_i 都是射影模，则称 C 为 M的**射影化解序列**.

我们有下面的定理：

定理9.3 设C,ε 是M上的射影复合形，C',ε' 是 M' 的化解序列，以及 $\mu: M\to M'$ 是模映射。则存在映射 $\alpha: C\to C'$，使$\mu\varepsilon=\varepsilon'\alpha_0$。更进一步说，如果存在另一个 $\beta: C\to C'$，使 $\mu\varepsilon=\varepsilon'\beta_0$，则 α 必与 β 同伦(即 $\alpha\sim\beta$)，$\bar{\alpha}_n=\bar{\beta}_n(\forall n\geqslant 0)$。

证明 为了眉目清晰，我们作下图：

$$\begin{array}{ccccccccccccccc}
\cdots\longrightarrow & C_n & \xrightarrow{d_n} & C_{n-1} & \xrightarrow{d_{n-1}} & C_{n-2} & \longrightarrow\cdots\longrightarrow & C_1 & \xrightarrow{d_1} & C_0 & \xrightarrow{\varepsilon} & M & \longrightarrow 0 \\
& \downarrow{\scriptstyle\alpha_n} & \swarrow{\scriptstyle s_{n-1}} & \downarrow{\scriptstyle\alpha_{n-1}} & \swarrow{\scriptstyle s_{n-2}} & \downarrow{\scriptstyle\alpha_{n-2}} & & \downarrow{\scriptstyle\alpha_1} & \swarrow{\scriptstyle s_0} & \downarrow{\scriptstyle\alpha_0} & \searrow{\scriptstyle\mu\varepsilon} & \downarrow{\scriptstyle\mu} & \\
\cdots\longrightarrow & C'_n & \xrightarrow{d'_n} & C'_{n-1} & \xrightarrow{d'_{n-1}} & C'_{n-2} & \longrightarrow\cdots\longrightarrow & C'_1 & \xrightarrow{d'_1} & C'_0 & \xrightarrow{\varepsilon'} & M' & \longrightarrow 0
\end{array}$$

图中实线部分已给定，虚线部分为待定。

因为 C_0 为射影模，ε'_1 为满射，所以按照射影模的定义，存在α_0，使

$$\varepsilon' \alpha_0 = \mu\varepsilon.$$

应用数学归纳法，设已作出$\alpha_0, \alpha_1, \cdots, \alpha_{n-1}$，使

$$\alpha_0 d_1 = d'_1 \alpha_1, \quad \cdots, \quad \alpha_{n-2} d_{n-1} = d'_{n-1} \alpha_{n-1}.$$

现在我们要作α_n。考虑

$$\alpha_{n-1} d_n: C_n \to C'_{n-1}.$$

因为C'，ε'是M'的化解序列，即(C', d')是正合的，所以有

$$\operatorname{im} d'_n = \ker d'_{n-1}.$$

已知

$$d'_{n-1}(\alpha_{n-1} d_n) = \alpha_{n-2} d_{n-1} d_n = 0,$$

令 $K = \operatorname{im}(\alpha_{n-1} d_n)$，则有

$$\alpha_{n-1} d_n: C_n \to K \subset C'_{n-1},$$

$$d'_{n-1}(K) = 0, \quad K \subset \ker d'_{n-1},$$

所以 $K \subset \operatorname{im} d'_n$。也即有下图：

$$\begin{array}{ccccc} & & C_n & & \\ & \swarrow^{\alpha_n} & \downarrow {\scriptstyle \alpha_{n-1} d_n} & & \\ C'_n & \xrightarrow{d'_n} & \operatorname{im} d'_n & \longrightarrow & 0 \end{array}$$

因为 C_n 是射影模，所以存在 α_n，使

$$d'_n \alpha_n = \alpha_{n-1} d_n.$$

现设有一个β，与α有同样的性质。我们要证明α与β同伦。按照同伦的定义，我们要定义出 $s_0, s_1, \cdots, s_n, \cdots$，使

$$s_i: C_i \to C'_{i+1},$$

$$\alpha_i - \beta_i = d'_{i+1} s_i + s_{i-1} d_i \quad (s_{-1} = 0),$$

与上面的证法类似，先考虑 $\alpha_0 - \beta_0$，由于

$$\varepsilon'(\alpha_0-\beta_0)=\mu\varepsilon-\mu\varepsilon=0,$$

即

$$\operatorname{im}(\alpha_0-\beta_0)\subset\ker\varepsilon'=\operatorname{im}d_1'.$$

所以存在下图：

$$\begin{array}{ccccc} & & C_0 & & \\ & \swarrow^{s_0} & \downarrow{\scriptstyle \alpha_0-\beta_0} & & \\ C_1' & \xrightarrow{d_1'} & \operatorname{im} d_1' & \longrightarrow & 0 \end{array}$$

因为C_0是射影模，所以存在 s_0，使

$$\alpha_0-\beta_0=d_1's_0.$$

应用数学归纳法，设已求出 $s_0,s_1,\cdots,s_{n-1}$，现在来求 s_n。考虑

$$\gamma=\alpha_n-\beta_n-s_{n-1}d_n:\ C_n\to C_n'.$$

我们有

$$\begin{aligned} d_n'\gamma&=d_n'\alpha_n-d_n'\beta_n-d_n's_{n-1}d_n=\alpha_{n-1}d_n-\beta_{n-1}d_n-d_n's_{n-1}d_n\\ &=(\alpha_{n-1}-\beta_{n-1}-d_n's_{n-1})d_n=s_{n-1}d_{n-1}d_n=0, \end{aligned}$$

所以 $\operatorname{im}\gamma\subset\ker d_n'=\operatorname{im}d_{n+1}'$。于是有下图：

$$\begin{array}{ccccc} & & C_n & & \\ & \swarrow^{s_n} & \downarrow{\scriptstyle \gamma} & & \\ C_{n+1}' & \xrightarrow{d_{n+1}'} & \operatorname{im} d_{n+1}' & \longrightarrow & 0 \end{array}$$

因为 C_n 是射影模，所以存在 s_n，使

$$\alpha_n-\beta_n-s_{n-1}d_n=\gamma=d_{n+1}'s_n. \quad \blacksquare$$

例9 我们举一个几何学的例子。任取一个平滑的曲面

$$f(x,y,z)=0.$$

平滑的条件即f_x, f_y, f_z在曲面上任一点不同时为零。于是通过曲面上的任意点 $P=(a,b,c)$，存在一个唯一的切面 T_P:

$$(X-a)f_x+(Y-b)f_y+(Z-c)f_z=0.$$

这些切面构成一个**切束**。

设曲面的定义方程式是代数方程式。读者不妨设想它是单位球面 $x^2+y^2+z^2-1=0$。令$R=\mathbf{R}[x,y,z]/(f(x,y,z))$，以及

$$\sigma: M=Ru\oplus Rv\oplus Rw\rightarrow R,$$

$$\sigma(u)=f_x,\quad \sigma(v)=f_y,\quad \sigma(w)=f_z.$$

又令$T=\ker(\sigma)$，$N=(f_xu+f_yv+f_zw)R$。我们可以证明T即切束，N即法线束。平滑的条件可以写成下式:

$$(f,f_x,f_y,f_z)=1,$$

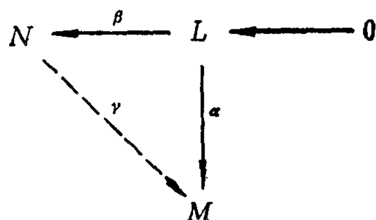
也即在R中$(f_x,f_y,f_z)=1$。所以σ是满射。而R是自由R模，故是射影模，于是存在 $\gamma: R\rightarrow M$，使 $\sigma\gamma=1_R$。所以

$$M=\gamma(R)\oplus T\approx N\oplus T,$$

于是得出切束是射影模。▎

同调代数论中，我们常用"共轭化"的方法：反转箭头。例如，我们把射影模定义中的箭头一律反转，则得出如下的定义。

定义9.9 如果对于任意模映射 $\alpha: L\rightarrow M$，以及任意模单射 $\beta: L\rightarrow N$，必有模映射 $\gamma: N\rightarrow M$，使$\alpha=\gamma\beta$，则称M是**内射模**。换言之，在下面的图形中:



虚线部分可用γ补足，使此图形为可交换的。

我们把定义 9.6 共轭化，得出下面的定义。

定义9.10 令M为R模。对于负复合形(C,d)：

$$0 \longrightarrow C^0 \xrightarrow{d^0} C^1 \xrightarrow{d^1} \cdots \longrightarrow C^{n-1} \xrightarrow{d^{n-1}} C^n \longrightarrow \cdots,$$

如果有一映射 ε: $M \to C^0$, 使 $d^0 \varepsilon = 0$, 则称(C,d)为M **下的复合形**，ε 为 **投入映射**。如果下面的序列是正合的，则称C是M**的上化解序列**：

$$0 \longrightarrow M \xrightarrow{\varepsilon} C^0 \xrightarrow{d^0} C^1 \xrightarrow{d^1} \cdots \longrightarrow C^{n-1} \xrightarrow{d^{n-1}} C^n \longrightarrow \cdots.$$

更进一步说，如果所有的C^i都是内射模，则称C是M**的内射上化解序列**。

我们对定理9.3共轭化，得出下面的定理。

定理9.4 设C,ε是M下的内射复合形，C',ε'是M的上化解序列，以及μ: $M' \to M$是模映射。则存在映射α: $C' \to C$，使得$\varepsilon\mu = \alpha^0 \varepsilon'$。更进一步说，如果存在另一个具有同样性质的映射$\beta$: $C' \to C$，则α必与β同伦(即$\alpha \sim \beta$)，$\alpha^n = \beta^n (\forall n \geqslant 0)$。

证明 读者自证之。▌

讨论 任给模M，是否必存在一个内射上化解序列呢？我们考虑射影化解的第一步：

$$C_0 \xrightarrow{\varepsilon} M \longrightarrow 0,$$

反转箭头后，得出

$$0 \longrightarrow M \xrightarrow{\varepsilon} C^0,$$

此处ε是单射。换言之，能不能把任给的模M，嵌入一个内射模C^0？如果能作到这点，同法我们可以把$C^0/\varepsilon(M)$嵌入内射模C^1，于是作出下图：

$$\begin{array}{ccccccc} & & & & C^0/\varepsilon(M) & & \\ & & & \nearrow & & \searrow & \\ 0 \longrightarrow M & \xrightarrow{\varepsilon} & C^0 & & \dashrightarrow & & C^1 \end{array},$$

因此，内射上化解序列的存在性，归结成下面的定理。

定理9.5 任给模M，都可以嵌入一个内射模N。

此定理与后文无关，其证明又较复杂，所以不给出其证明。

给定一个短正合序列

$$0 \longrightarrow N \longrightarrow L \longrightarrow M \longrightarrow 0,$$

我们要建造N, L, M的射影化解序列C, D, E，使下面的图形

$$\begin{array}{ccccccccccc}
 & & 0 & & 0 & & & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & & & \downarrow & & \downarrow & & \\
\cdots & \longrightarrow & C_{i+1} & \longrightarrow & C_i & \longrightarrow & \cdots & \longrightarrow & C_0 & \xrightarrow{\varepsilon} & N & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & & & \downarrow{\scriptstyle i_0} & & \downarrow{\scriptstyle \alpha} & & \\
\cdots & \longrightarrow & D_{i+1} & \longrightarrow & D_i & \longrightarrow & \cdots & \longrightarrow & D_0 & \xrightarrow{\lambda} & L & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & & & \downarrow{\scriptstyle \pi_0} & \nearrow{\scriptstyle \rho} & \downarrow{\scriptstyle \beta} & & \\
\cdots & \longrightarrow & E_{i+1} & \longrightarrow & E_i & \longrightarrow & \cdots & \longrightarrow & E_0 & \xrightarrow{\mu} & M & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & & & 0 & & 0 & &
\end{array}$$

为可交换的，以及每一直列都是正合的(请参考定理9.1)。我们先任取N的射影化解序列C及M的射影化解序列E，然后逐步地建造D_i。令

$$D_0 = C_0 \oplus E_0,$$

i_0为嵌入映射，π_0为投影映射。因为β是满射，E_0是射影模，所以存在映射

$$\rho: E_0 \to L,$$

使

$$\beta\rho = \mu.$$

我们定义λ如下：

$$\lambda(c_0, e_0) = \alpha\varepsilon(c_0) + \rho(e_0).$$

不难看出，

$$\lambda i_0(c_0)=\lambda(c_0,0)=\alpha\varepsilon(c_0),$$
$$\beta\lambda(c_0,e_0)=\beta\alpha\varepsilon(c_0)+\beta\rho(e_0)=\mu\pi_0(c_0,e_0).$$
所以，此部分图形是可交换的。我们现在要证明 λ 是满射。任取 $l\in L$。因为
$$\operatorname{im}\beta=M=\operatorname{im}\mu,$$
所以存在 $e_0\in E_0$，使 $\beta(l)=\mu(e_0)=\beta\rho(e_0)$，即
$$\beta(l-\rho(e_0))=0,\qquad l-\rho(e_0)\in\ker\beta=\operatorname{im}\alpha.$$
于是，存在 $n\in N$，使
$$l-\rho(e_0)=\alpha(n).$$
令 c_0 适合 $\varepsilon(c_0)=n$，则有
$$\lambda(c_0,e_0)=\alpha\varepsilon(c_0)+\rho(e_0)=\alpha(n)+\rho(e_0)=l.$$
因此 λ 是满射。我们再建造 D_1。考虑下面的图形：

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \\
\cdots & \longrightarrow & C_1 & \longrightarrow & N' & \longrightarrow & 0\\
 & & \downarrow & & \downarrow{\scriptstyle i_0} & & \\
\cdots & \longrightarrow & D_1 & \longrightarrow & L' & \longrightarrow & 0\\
 & & \downarrow & & \downarrow{\scriptstyle \pi_0} & & \\
\cdots & \longrightarrow & E_1 & \longrightarrow & M' & \longrightarrow & 0\\
 & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & &
\end{array}$$

其中 $N'=\ker\varepsilon$，$L'=\ker\lambda$，$M'=\ker\mu$。我们仅须证明
$$0\longrightarrow N'\longrightarrow L'\longrightarrow M'\longrightarrow 0$$
是正合的，就可以再次运用上面 D_0 的作法，作出 D_1。显然，任取 $c_0\in\ker\varepsilon=N'$，则有
$$\lambda i_0(c_0)=\lambda(c_0,0)=\alpha\varepsilon(c_0)=0,$$
所以 $i_0(N')\subset L'$。自然，i_0: $N'\to L'$ 是单射。任取 $l'\in L'=\ker\lambda$，则有

$$\mu\pi_0(l') = \beta\lambda(l') = 0,$$

所以 $\pi_0(L') \subset M'$，也即 $\pi_0: L' \to M'$ 是一个映射。现在我们要说明 $\pi_0: L' \to M'$ 是一个满射。任取 $e_0 \in M' = \ker\mu$，则有

$$0 = \mu(e_0) = \beta(\rho(e_0)),$$

所以
$$\rho(e_0) \in \ker\beta = \text{im}\,\alpha.$$

即存在 $n \in N$，$c_0 \in C_0$，使

$$\rho(e_0) = \alpha(n), \qquad \varepsilon(c_0) = n.$$

令 $l' = (-c_0, e_0)$，则有

$$\lambda(l') = -\alpha\varepsilon(c_0) + \rho(e_0) = -\alpha(n) + \rho(e_0) = 0,$$

即 $l' \in \ker\lambda = L'$，且

$$\pi_0(l') = e_0.$$

所以 $\pi_0: L' \to M'$ 是满射。

最后一步，我们要证明 $\ker\pi_0 = \text{im}\,\varepsilon_0$。因 $\pi_0 i_0 = 0: C_0 \to E_0$，所以 $\pi_0 i_0 = 0: N' \to M'$。如此得出

$$\text{im}\, i_0 \subset \ker\pi_0.$$

反之，任取 $l' = (c_0, e_0) \in L'$，适合 $\pi_0(l') = 0$，即有 $e_0 = 0$。于是

$$\lambda(c_0, 0) = \alpha\,\varepsilon(c_0) = 0.$$

因为 α 是单射，所以必有 $\varepsilon(c_0) = 0$，即 $c_0 \in \ker\varepsilon = N'$。故

$$l' = (c_0, 0) = i_0(c_0) \in \text{im}\, i_0.$$

综上所述，我们给出下面的定义及定理。

定义9.11 任给一个短正合序列 $0 \longrightarrow N \longrightarrow L \longrightarrow M \longrightarrow 0$。上文所讨论的射影化解序列的短正合列 $0 \longrightarrow C \longrightarrow D \longrightarrow E \longrightarrow 0$ 称为短正合序列 $0 \longrightarrow N \longrightarrow L \longrightarrow M \longrightarrow 0$ **的射影化解序列**。

定理9.6 任给一个短正合序列 $0 \longrightarrow N \longrightarrow L \longrightarrow M \longrightarrow 0$，都必存在它的射影化解序列 $0 \longrightarrow C \longrightarrow D \longrightarrow E \longrightarrow 0$。

习　　题

1．证明 R 模 M 是有限生成的射影模的充要条件是：它是具

有有限基的自由R模F的直和因子，即存在F的子模G，使得

$$F = M \oplus G.$$

2. 设M_i ($i \in I$, I为指标集)是射影模。证明$\bigoplus_{i \in I} M_i$也是射影模。

3. 设e是环R的一个幂等元素：$e^2 = e$。证明eR是射影R模。

4. 设$M_i (i \in I)$是内射模，证明$\prod_{i \in I} M_i$也是内射模。

5. 证明每个R模M都与一自由R模F的某个商模同构。

6. 给定两个影射R模M, N，证明存在一个自由R模F，使得

$$M \oplus F \approx N \oplus F,$$

且两者都是自由R模。

7. 证明$\mathbf{Q}$不是自由$\mathbf{Z}$模。

8. 设M, N是射影R模，且下面两个序列正合：

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

$$0 \longrightarrow N' \longrightarrow N \longrightarrow M'' \longrightarrow 0$$

证明：$M \oplus N' \approx N \oplus M'$。

9. 证明主理想整环R上的射影模都是自由模。

10. 设M是环$\mathbf{Z}$内由6, 8生成的理想。把M看作$\mathbf{Z}$模，试求M的两个不同的自由化解序列。

11. 给定正复合形

$$\cdots \longrightarrow C_n \longrightarrow C_{n-1} \longrightarrow \cdots \longrightarrow C_1 \longrightarrow C_0 \longrightarrow 0.$$

证明：$H_n(C) = 0 (n \geqslant 1)$的充要条件是下面的序列正合：

$$\cdots \longrightarrow C_n \longrightarrow C_{n-1} \longrightarrow \cdots \longrightarrow C_1 \longrightarrow C_0 \longrightarrow H_0(C) \longrightarrow 0.$$

12. 设

$$\cdots \longrightarrow C_n \longrightarrow C_{n-1} \longrightarrow \cdots \longrightarrow C_1 \longrightarrow C_0$$

是一个射影正复合形，又设有正复合形

$$\cdots \longrightarrow D_n \longrightarrow D_{n-1} \longrightarrow \cdots \longrightarrow D_1 \longrightarrow D_0,$$

其同调模$H_n(D)=0(n\geqslant 1)$。那么，对$H_0(C)$到$H_0(D)$的每个模映射φ，都存在C到D的映射α，使得φ由α诱导出，即

$$\varphi=\alpha_0.$$

且如果C到D的两个映射α,β都诱导出φ，则$\alpha\sim\beta$。

13. 证明题12的共轭(或称对偶)命题。

§4 Ext

任给两个R模M及A，令

$$\mathrm{Hom}(M,A)=\{\sigma:\sigma\text{ 为 }M\to A\text{ 的模映射}\}.$$

我们自然可以引入下面的代数运算：对于$f_1,f_2\in\mathrm{Hom}(M,A)$，$r_1,r_2\in R$，定义

$$(r_1f_1+r_2f_2)(m)=r_1(f_1(m))+r_2(f_2(m))\in A,\qquad \forall m\in M.$$

在这种运算下，$\mathrm{Hom}(M,A)$显然是R模。如果我们要着重标明环R，以免混淆，则往往用$\mathrm{Hom}_R(M,A)$代替$\mathrm{Hom}(M,A)$。

令C,ε是模M的一个射影化解序列，即有

$$0\longleftarrow M\xleftarrow{\varepsilon}C_0\xleftarrow{d_1}C_1\longleftarrow\cdots\xleftarrow{d_n}C_n\longleftarrow\cdots.$$

我们可以用ε定义如下的映射ε^*：

$$\varepsilon^*:\mathrm{Hom}(M,A)\to\mathrm{Hom}(C_0,A),$$

$$\varepsilon^*(f)=f\varepsilon.$$

请注意，箭头的方向反转了。不难验证ε^*确是模映射。同法我们可以考虑$d_1^*,d_2^*,\cdots,d_n^*,\cdots$。于是得出下面的负复合形：

$$0\longrightarrow\mathrm{Hom}(C_0,A)\xrightarrow{d_1^*}\mathrm{Hom}(C_1,A)\longrightarrow\cdots$$
$$\xrightarrow{d_n^*}\mathrm{Hom}(C_n,A)\longrightarrow\cdots.$$

它是一个复合形的原因是

$$d_{n+1}^*d_n^*(g)=d_{n+1}^*(gd_n)=gd_nd_{n+1}=0,$$
$$\forall g\in\mathrm{Hom}(C_{n-1},A),\quad n=1,2,\cdots$$

令其 i 阶上同调模为 $H^i(C,A)$. 我们需要应用定理 9.3 来证明 $H^i(C,A)$与C无关。换言之，设C', ε'是M的另一个射影化解序列，则必有

$$H^i(C,A) \approx H^i(C',A), \qquad \forall i = 0,1,2,\cdots.$$

证法如下。根据定理9.3，存在 α_i, β_i，使下图

$$\begin{array}{ccccccccccc}
\cdots \longrightarrow & C'_n & \longrightarrow \cdots \longrightarrow & C'_1 & \longrightarrow & C'_0 & \longrightarrow & M & \longrightarrow & 0 \\
& {\scriptstyle\beta_n}\uparrow\downarrow{\scriptstyle\alpha_n} & & {\scriptstyle\beta_1}\uparrow\downarrow{\scriptstyle\alpha_1} & & {\scriptstyle\beta_0}\uparrow\downarrow{\scriptstyle\alpha_0} & & \| & & \\
\cdots \longrightarrow & C_n & \longrightarrow \cdots \xrightarrow{d_2} & C_1 & \xrightarrow{d_1} & C_0 & \longrightarrow & M & \longrightarrow & 0 \\
& \downarrow{\scriptstyle\alpha_n\beta_n} & & \downarrow{\scriptstyle\alpha_1\beta_1} & & \downarrow{\scriptstyle\alpha_0\beta_0} & & \| & & \\
\cdots \longrightarrow & C_n & \longrightarrow \cdots \longrightarrow & C_1 & \longrightarrow & C_0 & \longrightarrow & M & \longrightarrow & 0
\end{array}$$

的上两行交换。于是从中间一行到下面一行存在映射 $\{\alpha_i\beta_i\}$。另一方面，下两行之间自然有一等同恒射 1，故

$$\alpha_i\beta_i \sim 1.$$

即存在映射 s_i，使

$$\alpha_i\beta_i = 1 + s_{i-1}d_i + d_{i+1}s_i.$$

由此立得

$$(\alpha_i\beta_i)^* = 1^* + d_i^* s_{i-1}^* + s_i^* d_{i+1}^*.$$

参考下图

$$\begin{array}{ccccccc}
\cdots \longrightarrow & \mathrm{Hom}(C_{i-1},A) & \xrightarrow{d_i^*} & \mathrm{Hom}(C_i,A) & \xrightarrow{d_{i+1}^*} & \mathrm{Hom}(C_{i+1},A) & \longrightarrow \cdots \\
& \downarrow{\scriptstyle(\alpha_{i-1}\beta_{i-1})^*} & \swarrow{\scriptstyle s_{i-1}^*} & \downarrow{\scriptstyle(\alpha_i\beta_i)^*} & \swarrow{\scriptstyle s_i^*} & \downarrow{\scriptstyle(\alpha_{i+1}\beta_{i+1})^*} & \\
\cdots \longrightarrow & \mathrm{Hom}(C_{i-1},A) & \xrightarrow{d_i^*} & \mathrm{Hom}(C_i,A) & \xrightarrow{d_{i+1}^*} & \mathrm{Hom}(C_{i+1},A) & \longrightarrow \cdots
\end{array}$$

所以我们有$(\alpha_i\beta_i)^* \sim 1^*$.于是对上同调模 H^i 而言,

$$\widetilde{(\alpha_i\beta_i)^*} = \tilde{1}^*.$$

也即

$$\widetilde{(\alpha_i\beta_i)^*} = \widetilde{\beta_i^*}\widetilde{\alpha_i^*}: H^i(C,A) \longrightarrow H^i(C,A)$$

是一同构映射。由此立得 $\widetilde{\alpha_i^*}$ 是单射，$\widetilde{\beta_i^*}$ 是满射。在上面的考虑中，我们交换 α_i,β_i，也即考虑 $\beta_i\alpha_i: C'_i\to C'_i$，则同法可得：$\widetilde{\beta_i^*}$ 是单射，$\widetilde{\alpha_i^*}$ 是满射。于是我们证明了

$$\widetilde{\alpha_i^*}: H^i(C,A)\approx H^i(C',A).$$

我们给出如下的定义。

定义9.12 任给二R模M,A，任取M的一个射影化解序列C,ε，我们定义

$$\mathrm{Ext}_R^i(M,A)=H^i(C,A)=H^i(\mathrm{Hom}_R(M,A)).$$

讨论 1）如上面所指出的，$\mathrm{Ext}_R^i(M,A)$ 与射影化解序列的选取无关。

2）Ext_R^i 的原来定义是"用M得出的A的i次扩充所构成的模"，这比较复杂。因此，我们采用了上面那个定义。请注意 Ext 即 extension 的头三个字母。

3）$\mathrm{Ext}_R^0(M,A)\approx\mathrm{Hom}_R(M,A)$。原因如下：首先，按照定义，我们知道

$$\mathrm{Ext}_R^0(M,A)=\ker d_1^*.$$

其次，已知下面的序列是正合的：

$$C_1\xrightarrow{d_1}C_0\xrightarrow{\varepsilon}M\longrightarrow 0,$$

考虑与它相应的序列

$$\mathrm{Hom}(C_1,A)\xleftarrow{d_1^*}\mathrm{Hom}(C_0,A)\xleftarrow{\varepsilon^*}\mathrm{Hom}(M,A)\longleftarrow 0.$$

我们要证明它也是正合的。证明了这一点之后，我们立得

$$\mathrm{Ext}_R^0(M,A)=\ker d_1^*=\mathrm{im}\,\varepsilon^*\approx\mathrm{Hom}(M,A).$$

证法如下：

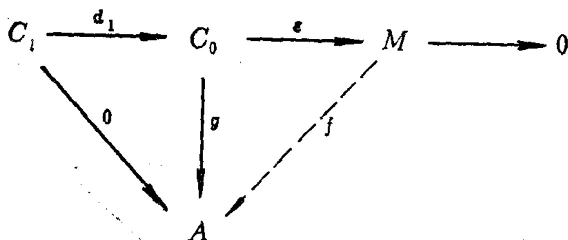
(a) ε^*是单射。原因是

$$\begin{aligned}\varepsilon^*(f)=0&\Longleftrightarrow f\varepsilon(c)=0, &&\forall c\in C_0\\&\Longleftrightarrow f(m)=0, &&\forall m\in M(\text{因}\varepsilon(C_0)=M)\\&\Longleftrightarrow f=0.\end{aligned}$$

(b) $\mathrm{im}\,\varepsilon^*=\ker d_1^*$。原因是：首先，

$$d_1^*\varepsilon^*(f)=f\,\varepsilon\,d_1=f\cdot 0=0,$$

所以 $\mathrm{im}\,\varepsilon^*\subset\ker d_1^*$。其次，任取 $g\in\ker d_1^*$，见下图：



我们要找一个 f，使上面的图可交换。任取 $m\in M$，令 $\varepsilon(c_0)=m$。定义

$$f(m)=g(c_0).$$

如果取不同的 $c_0'=c_0+d_1(c_1)$，则

$$f(m)=g(c_0+d_1(c_1))=g(c_0)+gd_1(c_1)=g(c_0).$$

所以，对所有可取的 c_0，$f(m)$ 是唯一确定的，即 f 是一个定义良好的映射。于是，不难看出 $g=f\varepsilon=\varepsilon^*(f)\in\mathrm{im}\,\varepsilon^*$，即有

$$\mathrm{im}\,\varepsilon^*=\ker d_1^*.$$

4）定义9.12给出了一个典范的方法：自一化解序列 (C,d)，得另一复合形 $(\mathrm{Hom}(C,A),d^*)$，又导出它的同调模 $\mathrm{Ext}_R^i(M,A)$。这是导出函子的方法。自然，如果导出的同调模

$$\mathrm{Ext}_R^i(M,A)\quad(i\geqslant 1)$$

都是零，换句话说，如果复合形 $(\mathrm{Hom}(M,A),d^*)$ 是正合的，则这个方法的意义将大为减少了。我们举出下面的例10，说明一般导出的同调模不是零。

例10 考虑 Z/mZ 的下面的自由化解序列（当然是射影化解序列）

$$0\longrightarrow Z\xrightarrow{m}Z\xrightarrow{\tau}Z/mZ\longrightarrow 0,$$

此处 m: $Z\to Z$ 表示映射 $m(n)=mn(\forall n\in Z)$，τ 是典型映射。任给 Z 模 A（即一交换群），我们得出

$$0 \longleftarrow A/mA \xleftarrow{\Delta^*} \mathrm{Hom}(Z, A) \xleftarrow{m^*} \mathrm{Hom}(Z, A)$$
$$\xleftarrow{\tau^*} \mathrm{Hom}(Z/mZ, A) \longleftarrow 0.$$

因为任给一个 $a \in A$，则 $f(1)=a$ 引生出 $\mathrm{Hom}(Z,A)$ 中的一个元素 f，而且 f 是由 $f(1)$ 唯一确定的，所以

$$\mathrm{Hom}(Z, A) \approx A, \quad m^*\mathrm{Hom}(Z, A) \approx mA.$$

因此上面得出的复合形是正合的。这也就是说

$$\mathrm{Ext}^1_Z(Z/mZ, A) \neq 0.$$

例11 参考例8。我们取 $R=C[x,y]$，$g(x,y)$ 与 $h(x,y)$ 无公因子，$N=(g(x,y),h(x,y))$。则有下列的自由化解序列

$$0 \longrightarrow R \xrightarrow{\begin{bmatrix} h \\ -g \end{bmatrix}} R \oplus R \xrightarrow{[g \ \ h]} N \longrightarrow 0.$$

此时 $R \oplus R$ 的元素都写成直列

$$\begin{bmatrix} a_1 \\ a_2 \end{bmatrix}.$$

我们考虑 $H^1(N,R)$。先取下面的复合形

$$0 \longleftarrow \mathrm{Hom}_R(R,R) \xleftarrow{\begin{bmatrix} h \\ -g \end{bmatrix}^*} \mathrm{Hom}_R(R \oplus R, R) \longleftarrow 0.$$

于是

$$H^0(N,R) = \ker\begin{bmatrix} h \\ -g \end{bmatrix}^* \Big/ (0) \approx \ker\begin{bmatrix} h \\ -g \end{bmatrix}^*,$$

$$H^1(N,R) = \mathrm{Hom}_R(R,R) \Big/ \mathrm{im}\begin{bmatrix} h \\ -g \end{bmatrix}^*.$$

进一步实际计算。取 $f \in \mathrm{Hom}_R(R \oplus R, R)$，设

$$f\left(\begin{bmatrix} 1 \\ 0 \end{bmatrix}\right) = f_1, \quad f\left(\begin{bmatrix} 0 \\ 1 \end{bmatrix}\right) = f_2,$$

则

$$\begin{bmatrix} h \\ -g \end{bmatrix}^*(f)=0 \Longleftrightarrow \left(\begin{bmatrix} h \\ -g \end{bmatrix}^*(f)\right)(1)=0$$

$$\Longleftrightarrow \left(f\begin{bmatrix} h \\ -g \end{bmatrix}\right)(1)=0$$

$$\Longleftrightarrow hf_1-gf_2=0 \Longleftrightarrow f_1=sg,\ f_2=sh \Longleftrightarrow f=s\sigma,$$

其中 $s\in R$, $\sigma\left(\begin{bmatrix} 1 \\ 0 \end{bmatrix}\right)=g$, $\sigma\left(\begin{bmatrix} 0 \\ 1 \end{bmatrix}\right)=h$. 所以

$$H^0(N,R)\approx\ker\begin{bmatrix} h \\ -g \end{bmatrix}^*=R\sigma\approx R.$$

现在计算 $H^1(N,R)$. 取 $1_R\in \mathrm{Hom}_R(R,R)$ 为

$$1_R(r)=r, \qquad \forall r\in R.$$

则有 $\mathrm{Hom}_R(R,R)=R\cdot 1_R\approx R$. 令 π_1,π_2 定义如下

$$\pi_1\left(\begin{bmatrix} 1 \\ 0 \end{bmatrix}\right)=1,\quad \pi_1\left(\begin{bmatrix} 0 \\ 1 \end{bmatrix}\right)=0,\quad \pi_2\left(\begin{bmatrix} 1 \\ 0 \end{bmatrix}\right)=0,\quad \pi_2\left(\begin{bmatrix} 0 \\ 1 \end{bmatrix}\right)=1.$$

我们立得

$$f=f_1\pi_1+f_2\pi_2,$$

$$\left(\begin{bmatrix} h \\ -g \end{bmatrix}^*(f)\right)(1)=\left(f\begin{bmatrix} h \\ -g \end{bmatrix}\right)(1)$$

$$=f\left(\begin{bmatrix} h \\ -g \end{bmatrix}(1)\right)=f_1h-f_2g.$$

所以
$$\mathrm{im}\begin{bmatrix} h \\ -g \end{bmatrix}^*\approx(g,h)=N\subset R.$$

即有
$$H^1(N,R)\approx R/N.$$

引理 在下列的短正合列中，如果 E_n 是射影模：

$$(*)\qquad 0\longrightarrow C_n\xrightarrow{i}D_n\underset{j}{\overset{\pi}{\rightleftarrows}}E_n\longrightarrow 0,$$

则我们恒有

$$0 \longleftarrow \mathrm{Hom}(C_n, N) \xleftarrow{i^*} \mathrm{Hom}(D_n, N) \xleftarrow{\pi^*} \mathrm{Hom}(E_n, N) \longleftarrow 0$$

是正合的。

证明 我们应证明三点：1) π^*是单射；2) $\mathrm{im}\,\pi^* = \ker i^*$；3) i^*是满射。前两点在一般情形下(即不要求 E_n 是射影模)都是正确的，读者自证之。我们来证 3)。

因为 E_n 是射影模，所以序列(*)的虚线部分可以用 j 足，使 $\pi j = 1$。不难看出

$$D_n = i(C_n) \oplus j(E_n).$$

任取 $h \in \mathrm{Hom}(C_n, N)$ 令

$$g(i(c_n), j(e_n)) = h(c_n) \quad (\forall c_n \in C_n,\ e_n \in E_n),$$

则 $g \in \mathrm{Hom}(D_n, N)$，而且 $i^*(g) = h$。所以 i^* 是一个满射。∎

定理9.7 设有一个短正合序列

$$0 \longrightarrow N \longrightarrow L \longrightarrow M \longrightarrow 0.$$

则有下面的长正合序列

$$0 \longrightarrow \mathrm{Ext}^0(M, A) \longrightarrow \mathrm{Ext}^0(L, A) \longrightarrow \mathrm{Ext}^0(N, A)$$

$$\xrightarrow{\Delta^*} \mathrm{Ext}^1(M, A) \longrightarrow \cdots \longrightarrow \mathrm{Ext}^i(N, A)$$

$$\xrightarrow{\Delta^*} \mathrm{Ext}^{i+1}(M, A) \longrightarrow \mathrm{Ext}^{i+1}(L, A) \longrightarrow \cdots.$$

证明 根据定理9.6，我们可以取此短正合序列的一个射影化解序列 $0 \longrightarrow C \longrightarrow D \longrightarrow E \longrightarrow 0$，即

$$\begin{array}{ccccccccc}
 & & 0 & & & & 0 & & 0 & & \\
 & & \downarrow & & & & \downarrow & & \downarrow & & \\
\cdots & \longrightarrow & C_n & \longrightarrow & \cdots & \longrightarrow & C_0 & \xrightarrow{\varepsilon} & N & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle i_n} & & & & \downarrow{\scriptstyle i_0} & & \downarrow{\scriptstyle \alpha} & & \\
\cdots & \longrightarrow & D_n & \longrightarrow & \cdots & \longrightarrow & D_0 & \xrightarrow{\lambda} & L & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \pi_n} & & & & \downarrow{\scriptstyle \pi_0} & & \downarrow{\scriptstyle \beta} & & \\
\cdots & \longrightarrow & E_n & \longrightarrow & \cdots & \longrightarrow & E_0 & \xrightarrow{\mu} & M & \longrightarrow & 0 \\
 & & \downarrow & & & & \downarrow & & \downarrow & & \\
 & & 0 & & & & 0 & & 0 & &
\end{array}$$

对此图取 Hom$(-,N)$，则得下图：

$$
\begin{array}{ccccccc}
 & & 0 & & & 0 & \\
 & & \uparrow & & & \uparrow & \\
\cdots\longleftarrow & & \mathrm{Hom}(C_n,N) & \longleftarrow\cdots\cdots\longleftarrow & & \mathrm{Hom}(C_0,N) & \longleftarrow 0\\
 & & \uparrow{\scriptstyle i_n^*} & & & \uparrow{\scriptstyle i_0^*} & \\
\cdots\longleftarrow & & \mathrm{Hom}(D_n,N) & \longleftarrow\cdots\cdots\longleftarrow & & \mathrm{Hom}(D_0,N) & \longleftarrow 0\\
 & & \uparrow{\scriptstyle \pi_n^*} & & & \uparrow{\scriptstyle \pi_0^*} & \\
\cdots\longleftarrow & & \mathrm{Hom}(E_n,N) & \longleftarrow\cdots\cdots\longleftarrow & & \mathrm{Hom}(E_0,N) & \longleftarrow 0\\
 & & \uparrow & & & \uparrow & \\
 & & 0 & & & 0 &
\end{array}
$$

我们仅须说明每一列都是正合的，便可用定理9.1导出本定理了。前面的引理正好证明了这一点。 ▌

应用上定理，我们可以得出射影模的同调代数论的定义，即下定理。

定理9.8 对任意模M而言，下面的三个性质是等同的：

1) M是射影模；

2) 对所有的$n\geqslant 1$及所有的模N，$\mathrm{Ext}^n(M,N)=0$；

3) 对所有的模N，$\mathrm{Ext}^1(M,N)=0$。

证明 1)$\Longrightarrow$2)。已知M是射影模，所以下面的序列是M的射影化解序列：

$$0\longrightarrow M\longrightarrow M\longrightarrow 0,$$

即取$C_0=M$，$C_1=C_2=\cdots=0$。于是序列

$$0\longrightarrow \mathrm{Hom}(C_0,N)\longrightarrow \mathrm{Hom}(C_1,N)\longrightarrow\cdots$$

即是
$$0\longrightarrow \mathrm{Hom}(M,N)\longrightarrow 0\longrightarrow\cdots.$$

计算其同调模，立得2)．

2)$\Longrightarrow$3)。立得。

3)$\Longrightarrow$1)。我们任取一个短正合序列

$$0\longrightarrow K\xrightarrow{i} F\xrightarrow{\pi} M\longrightarrow 0,$$

此处F是自由模。应用定理9.7及性质3)，我们立得正合序列

$$0 \longrightarrow \mathrm{Ext}^0(M,K) \longrightarrow \mathrm{Ext}^0(F,K) \longrightarrow \mathrm{Ext}^0(K,K) \longrightarrow 0,$$

也即

$$0 \longrightarrow \mathrm{Hom}(M,K) \xrightarrow{\pi^*} \mathrm{Hom}(F,K) \xrightarrow{i^*} \mathrm{Hom}(K,K) \longrightarrow 0.$$

取 $1_K \in \mathrm{Hom}(K,K)$，则必存在 $f \in \mathrm{Hom}(F,K)$，使

$$i^*(f) = fi = 1_K.$$

令$M' = \ker f$，则有

$$0 \longrightarrow M' \xrightarrow{j} F \underset{i}{\overset{f}{\rightleftarrows}} K \longrightarrow 0,$$

其中 j 为嵌入映射。由此立得K是射影模，以及

$$F = j(M') \oplus i(K), \qquad M' \approx j(M') \approx F/i(K) \approx M.$$

所以，M是一个自由模的直和因子，也即是一个射影模。▌

讨论 本定理将在§6“同调维数”中推广。▌

我们也可以用内射上化解序列来定义Ext^i。

为了眉目清晰起见，我们先用内射上化解序列定义$\overline{\mathrm{Ext}}^i$，然后证明 $\mathrm{Ext}^i = \overline{\mathrm{Ext}}^i$。

定义9.13 令 D, ε 是A的一个内射上化解序列：

$$0 \longrightarrow A \xrightarrow{\varepsilon} D^0 \xrightarrow{\partial^0} D^1 \xrightarrow{\partial^1} D^2 \longrightarrow \cdots.$$

令 $\mathrm{Hom}(M,D)$为下面的复合形

$$0 \longrightarrow \mathrm{Hom}(M,D^0) \longrightarrow \mathrm{Hom}(M,D^1) \longrightarrow \cdots.$$

我们定义$\overline{\mathrm{Ext}}^i(M,A)$为它的 i 阶上同调模。

我们要证明：

定理9.9 $\mathrm{Ext}^i(M,A) \approx \overline{\mathrm{Ext}}^i(M,A)$。

证明 不难看出

$$\mathrm{Ext}^0(M,A) = \mathrm{Hom}(M,A) = \overline{\mathrm{Ext}}^0(M,A).$$

任取一个短正合序列如下（其中P是射影模）：

$$0 \longrightarrow K \xrightarrow{i} P \xrightarrow{\pi} M \longrightarrow 0.$$

应用定理9.8及定理9.7，我们得出

$$0 \longrightarrow \mathrm{Hom}(M,A) \xrightarrow{\pi^*} \mathrm{Hom}(P,A) \xrightarrow{i^*} \mathrm{Hom}(K,A)$$

$$\xrightarrow{\Delta^*} \mathrm{Ext}^1(M,A) \longrightarrow 0 \longrightarrow \mathrm{Ext}^1(K,A)$$

$$\xrightarrow{\Delta^*} \mathrm{Ext}^2(M,A) \longrightarrow 0 \longrightarrow \cdots.$$

用同样方法，不难得出

$$0 \longrightarrow \mathrm{Hom}(M, A) \xrightarrow{\pi^*} \mathrm{Hom}(P,A) \xrightarrow{i^*} \mathrm{Hom}(K,A)$$

$$\xrightarrow{\bar{\Delta}^*} \overline{\mathrm{Ext}}^1(M,A) \longrightarrow 0 \longrightarrow \overline{\mathrm{Ext}}^1(K,A)$$

$$\xrightarrow{\bar{\Delta}^*} \overline{\mathrm{Ext}}^2(M,A) \longrightarrow 0 \longrightarrow \cdots.$$

由此立得

$$\mathrm{Ext}^1(M,A) \approx \mathrm{Hom}(K,A)/i^*(\mathrm{Hom}(P,A)) \approx \overline{\mathrm{Ext}}^1(M,A),$$

$$\mathrm{Ext}^n(M,A) \approx \mathrm{Ext}^{n-1}(K,A), \quad \overline{\mathrm{Ext}}^n(M,A) \approx \overline{\mathrm{Ext}}^{n-1}(K,A).$$

应用数学归纳法，已知 $\mathrm{Ext}^{n-1}(K,A) \approx \overline{\mathrm{Ext}}^{n-1}(K,A)$，于是立得本定理。▌

与定理 9.8 相同的，我们可以证明下面的定理。

定理9.10 对任意模N而言，下面的三个性质是等同的：

1）N是内射模；

2）对所有的 $n \geqslant 1$ 及所有的模M，$\mathrm{Ext}^n(M,N)=0$；

3）对所有的模M，$\mathrm{Ext}^1(M,N)=0$。

习 题

1. 设有R模映射序列

$$M' \xrightarrow{u} M \xrightarrow{v} M'' \longrightarrow 0.$$

证明这个序列正合的充要条件是：对任意R模N，下面的序列正合

$$0 \longrightarrow \mathrm{Hom}(M'', N) \xrightarrow{v^*} \mathrm{Hom}(M, N) \xrightarrow{u^*} \mathrm{Hom}(M', N),$$

其中 u^*, v^*是由 u, v 诱导得出的。

2. 设有R模映射序列

$$0 \longrightarrow N' \xrightarrow{u} N \xrightarrow{v} N''.$$

证明这个序列正合的充要条件是：对任意R模M，下面的序列正合：

$$0 \longrightarrow \mathrm{Hom}(M, N') \xrightarrow{\bar{u}} \mathrm{Hom}(M, N) \xrightarrow{\bar{v}} \mathrm{Hom}(M, N''),$$

其中$\bar{u}$定义如下：$\forall f \in \mathrm{Hom}(M, N')$，其在$\bar{u}$下映成$\mathrm{Hom}(M, N)$内的$uf$；$\bar{v}$的定义方法相同。

3. 证明R模M是射影模的充要条件是：对任意的R模短正合序列

$$0 \longrightarrow A \xrightarrow{u} B \xrightarrow{v} C \longrightarrow 0,$$

下面的序列正合：

$$0 \longrightarrow \mathrm{Hom}(M, A) \xrightarrow{\bar{u}} \mathrm{Hom}(M, B) \xrightarrow{\bar{v}} \mathrm{Hom}(M, C) \longrightarrow 0,$$

其中$\bar{u}, \bar{v}$的定义同题2.

4. 令$R = D$为主理想整环，$a \in D$. 令$M = D/(a)$为R模，它的一个射影化解序列为

$$\cdots \longrightarrow 0 \longrightarrow D \longrightarrow D \longrightarrow M \longrightarrow 0,$$

其中$D \longrightarrow D$是乘a的映射，而$D \longrightarrow M$是典型映射. 对R模N，考虑$\mathrm{Hom}(D, N)$到N的映射如下：$\forall \eta \in \mathrm{Hom}(D, N)$，定义$\eta \mapsto \eta(1)$. 利用它们证明

$$\mathrm{Ext}^1(M, N) \approx N/aN,$$

并证明：若$N = D/(b)$，则

$$\mathrm{Ext}^1(M, N) \approx D/(a, b),$$

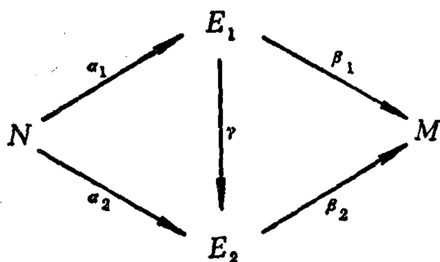
这里(a, b)表示a, b在D内生成的理想.

5. 设M, N是R模，如果R模E使下面序列正合：

$$0 \longrightarrow N \xrightarrow{\alpha} E \xrightarrow{\beta} M \longrightarrow 0,$$

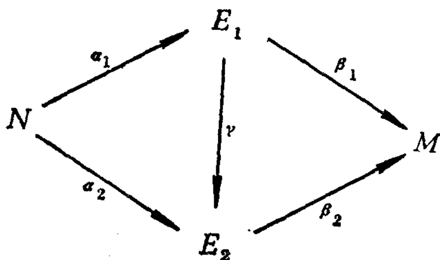
则称E是M关于N的一个扩充. 设E_1, E_2是两个扩充，γ是E_1到

E_2 的模映射，使下图交换：



证明 γ 必是一个模同构，并证明 R 模关于 N 的扩充 E 总是存在的。

6. 设 M, N 是 R 模，M 关于 N 的两个扩充 E_1 与 E_2 称为等价，若存在 E_1 到 E_2 的同构 γ，使下图交换：



命 $E(M,N)$ 表示 M 关于 N 的扩充的等价类所成的集合。证明 $E(M,N)$ 和 $\mathrm{Ext}^1(M,N)$ 之间存在一一对应。

7. 对 R 模 M_i, N $(i \in I)$，证明

(1) $\mathrm{Ext}^n(\bigoplus_{i \in I} M_i, N) \approx \prod_{i \in I} \mathrm{Ext}^n(M_i, N)$,

(2) $\mathrm{Ext}^n\left(N, \prod_{i \in I} M_i\right) \approx \prod_{i \in I} \mathrm{Ext}^n(N, M_i)$.

8. 证明：R 模 M 是内射模的充要条件是：对 R 的任意理想 I，

$$\mathrm{Ext}^1(R/I, M) = 0.$$

§5 张量积与 Tor

张量源出于物理学中计算物体内的张力。后来在微分几何学中有了广泛的应用。例如，三维空间的位移微分 ds 可以写成下式

$$ds^2 = \sum_{i,j} g_{ij} dx^i dx^j.$$

当我们变换坐标$\{x^i\} \to \{x^{*k}\}$时，

$$\begin{aligned} ds^2 &= \sum_{i,j} g_{ij} dx^i dx^j = \sum_{i,j,k,l} g_{ij} \frac{\partial x^i}{\partial x^{*k}} \frac{\partial x^j}{\partial x^{*l}} dx^{*k} dx^{*l} \\ &= \sum_{k,l} \left(\sum_{i,j} g_{ij} \frac{\partial x^i}{\partial x^{*k}} \frac{\partial x^j}{\partial x^{*l}} \right) dx^{*k} dx^{*l} \\ &= \sum_{k,l} g^*_{kl} dx^{*k} dx^{*l}, \end{aligned}$$

其中

$$g^*_{kl} = \sum_{i,j} g_{ij} \frac{\partial x^i}{\partial x^{*k}} \frac{\partial x^j}{\partial x^{*l}}.$$

此时，$\{g_{ij}\}$称为**共变张量**，而$\{dx^i\}$称为**反变张量**，因为它适合

$$dx^{*k} = \sum_i \frac{\partial x^{*k}}{\partial x^i} dx^i.$$

一般而言，取一向量空间 $V = \sum_i K e^i$，我们定义**张量积**

$$V \otimes V = \sum_{i,j} K e^i \otimes e^j,$$

适合下列公式：

$$\begin{aligned} &(v_1 + v_2) \otimes u = v_1 \otimes u + v_2 \otimes u, \\ &v \otimes (u_1 + u_2) = v \otimes u_1 + v \otimes u_2, \\ &(kv) \otimes u = v \otimes (ku) = k(v \otimes u), \end{aligned}$$

其中 $v, u, v_i, u_j \in V$，$k \in K$。任取 $w \in V \otimes V$，则 w 可以写成下式

$$w=\sum_{i,j}f_{ij}e^i\otimes e^j.$$

当我们进行下述坐标变换时：

$$e^i=\sum_k a^i_k e^{*k},$$

则有 $$w=\sum_{i,j,k,l}f_{ij}a^i_k a^j_l e^{*k}\otimes e^{*l}=\sum_{k,l}f^*_{kl}e^{*k}\otimes e^{*l},$$

此处 $$f^*_{kl}=\sum_{i,j}f_{ij}a^i_k a^j_l.$$

与前段有关 ds^2 的计算相比，可知$\{f_{ij}\}$即相当于共变张量$\{g_{ij}\}$.

在本节中，我们将要讨论任意的 R 模 M,N 的“张量积” $M\otimes_R N$.

定义9.14 $M\otimes_R N$ 即由符号 $m\otimes n$生成而且适合下列公式的 R 模：

$$(m_1+m_2)\otimes n=m_1\otimes n+m_2\otimes n,\quad m\otimes(n_1+n_2)=m\otimes n_1+m\otimes n_2,$$
$$(rm)\otimes n=m\otimes(rn)=r(m\otimes n),$$

其中 $m,m_1,m_2\in M$, $n,n_1,n_2\in N$, $r\in R$.

讨论 是否存在这样的 R 模 $M\otimes_R N$ 呢？于是，下面的定义9.14′较好。

定义9.14′ 取 $M\circ N$ 为由所有符号$m\circ n$生成的自由R模。再取K为由所有符号$(m_1+m_2)\circ n-m_1\circ n-m_2\circ n, m\circ(n_1+n_2)-m\circ n_1-m\circ n_2$, $(rm)\circ n-r(m\circ n)$, $m\circ(rn)-r(m\circ n)$ 生成的子模。令

$$M\circ N\xrightarrow{\sigma}M\circ N/K=M\otimes_R N,\qquad \sigma(m\circ n)=m\otimes n.$$

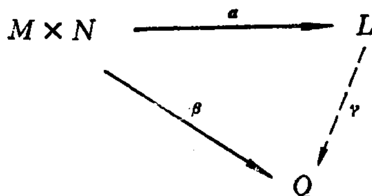
则立得 $M\otimes_R N$ 是一个 R 模。

讨论 上面的定义确实构造出了 $M\otimes_R N$，然而比较复杂。通常我们可以用下面的定理，得出张量积的又一个定义。

定理9.11 给定 R 模 M,N，则 $M\otimes_R N$ 是唯一能适合下面条件的 R 模 L（参考下图，见下页）：存在 $\alpha: M\times N\to L$ 为一双线

性映射，使得对于任意给定的模 Q 及双线性映射 $\beta: M\times N\to Q$。必存在唯一的模映射 $\gamma: L\to Q$，使

$$\gamma\alpha=\beta.$$



证明 令 $L=M\otimes_R N$，$\alpha: M\times N\to L$ 定义为

$$\alpha((m,n))=m\otimes n.$$

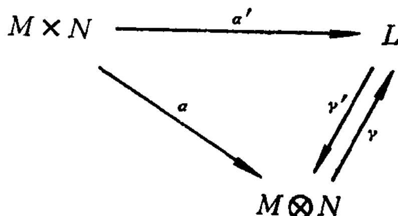
α 显然对 M 及 N 都是线性的，所以是双线性映射。定义

$$\pi: M\circ N\to M\times N,$$

$$\pi(m\circ n)=(m,n).$$

显然 π 是模映射。对于任给的模 Q 及双线性映射 $\beta: M\times N\to Q$，β 可以扩充为映射 $\tilde{\beta}: M\circ N\to M\times N\to Q$，即 $\tilde{\beta}=\beta\pi$。由于 β 是双线性的，所以 $\tilde{\beta}(K)=0$。于是 $\tilde{\beta}$ 诱导出 $M\otimes_R N=M\circ N/K$ 到 Q 的模映射 γ。显然 $\gamma\alpha=\beta$。又因为在 α 下 $M\otimes_R N$ 中的任一元素被 $M\times N$ 中的某些元素完全确定，不难看出，满足 $\gamma\alpha=\beta$ 的模映射 γ 是唯一的。

反之，设 L 适合本定理给出的条件。则有交换图：



(即取 $Q=M\otimes_R N$，$\beta=\alpha$，得到 γ'；又取 $Q=L$，$\beta=\alpha'$，得到 γ)，即有

$$\gamma'\alpha' = \alpha,\quad \gamma\alpha = \alpha',\quad \gamma\gamma'\alpha' = \alpha'.$$

但显然 1_L 满足 $1_L\alpha' = \alpha'$，由唯一性，即有 $\gamma\gamma' = 1_L$。同样，$\gamma\gamma' = 1_{M\otimes N}$。于是 γ, γ' 均为同构。▍

例12 1) 设 M, N 都是自由模，$M = \sum_i Re_i$，$N = \sum_j Rf_j$。不难看出，$M\otimes_R N = \sum_{i,j} Re_i\otimes f_j$。如果 R 是域，M, N 都是有限维向量空间，则有

$$\dim M\otimes_R N = (\dim M)(\dim N).$$

2) $m\otimes n = ?$ 这是一个含意不清的问题。我们举例说明这一点。取 $R = \boldsymbol{Z} \supset M = m\boldsymbol{Z}$，$N = \boldsymbol{Z}/m\boldsymbol{Z}$。$m\otimes\bar{1}$ 有如下两种不同的含意：

$$m\otimes\bar{1} \in \boldsymbol{Z}\otimes_{\boldsymbol{Z}} N \approx N;$$

$$m\otimes\bar{1} \in M\otimes_{\boldsymbol{Z}} N.$$

在第一种情形，$m\otimes\bar{1} = m(1\otimes\bar{1}) = 1\otimes m\bar{1} = 1\otimes 0 = 0$。在第二种情形，我们不能自由移动 m（因为 $1 \overline{\in} M$）。所以，在下面的同构作用下

$$\sigma: M\otimes_{\boldsymbol{Z}} N \approx N,$$
$$\sigma(lm\otimes\bar{1}) = l\,\bar{1},$$

我们有 $\sigma(m\otimes\bar{1}) = \bar{1} \neq 0$，即 $m\otimes\bar{1} \neq 0$。因此，在考虑 $m\otimes n$ 时，我们必须说明它在哪儿。

定理9.12 我们有下列的自然同构：

1) $M\otimes N \approx N\otimes M$: $m\otimes n \rightleftarrows n\otimes m$;

2) $(M\otimes N)\otimes L \approx M\otimes(N\otimes L)$: $(m\otimes n)\otimes l \rightleftarrows m\otimes(n\otimes l)$.

所以我们可以用 $M\otimes N\otimes L$ 表示 $(M\otimes N)\otimes L$ 或 $M\otimes(N\otimes L)$。

证明 读者自证之。▍

根据上面的定理，我们可以讨论 $M_1\otimes M_2\otimes\cdots\otimes M_n$，并不至于引起混淆。

与定义 $\mathrm{Ext}_R^i(M, N)$ 一样地，我们可以定义 $\mathrm{Tor}_i^R(M, N)$ 如

下：任取 N 的一个射影化解序列

$$0 \longleftarrow N \xleftarrow{\varepsilon} C_0 \xleftarrow{d_1} C_1 \longleftarrow \cdots \xleftarrow{d_n} C_n \longleftarrow \cdots,$$

对 M 取张量积，得出下面的复合形：

$$0 \longleftarrow M\otimes_R C_0 \xleftarrow{1\otimes d_1} M\otimes_R C_1 \xleftarrow{1\otimes d_2} M\otimes_R C_2 \longleftarrow \cdots,$$

其中，映射 $1\otimes d_n$ 是如下自然定义的：

$$(1\otimes d_n)(m\otimes c_n) = m\otimes d_n(c_n).$$

易于得出

$$(1\otimes d_{n-1})(1\otimes d_n) = 1\otimes d_{n-1}d_n = 1\otimes 0 = 0.$$

所以，上面的张量积序列确是一个复合形。我们对它取同调模 $H_i(M\otimes C)$。应用上节关于 $\mathrm{Ext}_R^i(C,N)$ 的讨论，不难看出，$H_i(M\otimes C)$ 与 N 的射影化解序列 C 无关。因此我们有下面的定义。

定义9.15 $\mathrm{Tor}_i^R(M,N) = H_i(M\otimes C)$。

讨论 $\mathrm{Tor}_0^R(M,N) = M\otimes_R N$。证法如下：我们已知

$$\mathrm{Tor}_0^R(M,N) = M\otimes_R C_0/\mathrm{im}(1\otimes d_1).$$

令 $L = M\otimes_R C_0/\mathrm{im}(1\otimes d_1)$。我们有下图：

$$\begin{array}{ccccccc}
0 & \longleftarrow & L & \xleftarrow{\pi} & M\otimes_R C_0 & \xleftarrow{1\otimes d_1} & M\otimes_R C_1 \\
 & & j\uparrow\downarrow i & \swarrow_{1\otimes\varepsilon} & & & \\
 & & M\otimes_R N & & & &
\end{array}$$

因为

$$(1\otimes\varepsilon)(1\otimes d_1) = 1\otimes\varepsilon d_1 = 1\otimes 0 = 0,$$

所以

$$\ker(1\otimes\varepsilon)\supset\mathrm{im}(1\otimes d_1) = \ker\pi.$$

于是自然定义出一个映射 i。又因 ε 是满射，任取 $(m,n)\in M\times N$，必有 $m\otimes c_0\in M\otimes_R C_0$，使 $(1\otimes\varepsilon)(m\otimes c_0) = m\otimes n$。设 c_0' 与 c_0 有同样的性质，则有

$$n=\varepsilon(c_0)=\varepsilon(c_0') \iff c_0-c_0'\in\ker\varepsilon=\operatorname{im} d_1$$
$$\iff \pi(m\otimes c_0)=\pi(m\otimes c_0').$$

于是我们可以定义一个双线性映射

$$a: M\times N\to L,$$
$$a((m,n))=\pi(m\otimes c_0).$$

根据定理9.11，必存在唯一的映射 j. 不难看出，$ij=1$，$ji=1$。立得 $M\otimes_R N\approx \operatorname{Tor}(M,N)$。 ▎

我们现在仿照上一节建立 $\operatorname{Tor}_i^R(M,N)$ 的性质。首先证明：

引理 在下列短正合序列中：

$$(*)\qquad 0\longleftarrow E_n \underset{j}{\overset{\pi}{\rightleftarrows}} D_n \overset{i}{\longleftarrow} C_n\longleftarrow 0,$$

如果 E_n 是射影模，则我们恒有

$$0\longleftarrow M\otimes_R E_n \overset{1\otimes\pi}{\longleftarrow} M\otimes_R D_n \overset{1\otimes i}{\longleftarrow} M\otimes_R C_n\longleftarrow 0$$

是正合的。

证明 我们应该证明三点：1) $1\otimes\pi$ 是满射；2) $\ker(1\otimes\pi)=\operatorname{im}(1\otimes i)$；3) $1\otimes i$ 是单射。在一般情形下(即不要求 E_n 是射影模)，前二者都是正确的。读者自证之。我们来证 3)。

因为 E_n 是射影模，所以序列$(*)$的虚线部分可以用 j 补足，使 $\pi j=1$。不难看出，$D_n=i(C_n)\oplus j(E_n)$。因此

$$M\otimes D_n=M\otimes i(C_n)\oplus M\otimes j(E_n).$$

显然

$$1\otimes i: M\otimes C_n\approx M\otimes i(C_n). \ ▎$$

与定理9.7的证法类似，我们可以证明：

定理9.13 设有一个短正合序列

$$0\longleftarrow N''\longleftarrow N\longleftarrow N'\longleftarrow 0,$$

则有下面的长正合序列：

$$0\longleftarrow \operatorname{Tor}_0^R(M,N'')\longleftarrow \operatorname{Tor}_0^R(M,N)\longleftarrow \operatorname{Tor}_0^R(M,N')$$
$$\longleftarrow \operatorname{Tor}_1^R(M,N'')\longleftarrow\cdots\longleftarrow \operatorname{Tor}_i^R(M,N')$$
$$\longleftarrow \operatorname{Tor}_{i+1}^R(M,N'')\longleftarrow \operatorname{Tor}_{i+1}^R(M,N)$$

$$\longleftarrow \mathrm{Tor}_{i+1}^R(M,N') \longleftarrow \cdots.$$

与定理9.9类似，我们可以取 M 的一个射影化解序列 C'，ε'，然后用它来定义 $\overline{\mathrm{Tor}}_i^R(M,N)$。不难看出

$$\overline{\mathrm{Tor}}_i^R(M,N) \approx \mathrm{Tor}_i^R(N,M).$$

我们又有下面的定理(证明略)。

定理9.14 $\mathrm{Tor}_i^R(M,N) = \mathrm{Tor}_i^R(N,M)$。

参考定理9.8，我们可以用同调代数论的方法，即 Ext_R^i 的性质来定义射影模。相应地，$\mathrm{Tor}_i^R(M,N)$定义了什么呢？为此，我们进行下面的讨论。

设 M 是自由模，$M = \oplus Re_i$。令 $x_j \in M$，适合下列的方程式

$$\sum_j r_j x_j = 0, \quad r_j \in R. \tag{1}$$

用$\{e_i\}$表出 x_j 如下：

$$x_j = \sum_i s_{ji} e_i, \quad s_{ji} \in R. \tag{2}$$

代入上式，立得

$$\sum_{i,j} r_j s_{ji} e_i = 0,$$

$$\sum_j r_j s_{ji} = 0, \quad i = 1, 2, \cdots. \tag{3}$$

定义9.16 如果在模M中，方程式(1)均可由(2)及(3)求解(此时$\{e_i\}$不必是M的R基)，则称M为**平模**。

讨论 自由模显然是平模。一般言之，平模可以理解成自由模的极限。

例13 1) Q 不是自由 Z 模，但显然是平 Z 模。

2) 令$M = C[x,y,z]/(z^2 - f(x,y)) \approx C[x,y] \oplus C[x,y]z$。则$M$是一个自由 $C[x,y]$模，所以是平$C[x,y]$模。从几何观点来看，$z^2 - f(x,y)$定义了复平面(相当于 $C[x,y]$)的一个复叠曲面，而这个复叠确实是"平"的。

3) 令$M = C[x,y,z]/(xz - y)$。视M为 $C[x,y]$模。显然

$$M \approx \boldsymbol{C}[x,y][y/x] = \boldsymbol{C}[x,y/x].$$

现在我们要证明M不是平 $\boldsymbol{C}[x,y]$模。考虑下面的方程式

$$xz - y\cdot 1 = 0, \quad z,1\in M, \ x,y\in R = \boldsymbol{C}[x,y].$$

如有下面的解：

$$z = \sum_i s_{i1}e_i, \quad e_i\in M, \ s_{i1}\in R,$$

$$1 = \sum_i s_{i2}e_i, \quad s_{i2}\in R,$$

$$xs_{i1} - ys_{i2} = 0, \quad i = 1,2,\cdots.$$

则立得 $x|s_{i2}$，即有

$$1\in(x)\subset \boldsymbol{C}[x,y/x].$$

此式显然是不可能成立的。于是M不是平 $\boldsymbol{C}[x,y]$ 模。从几何观点来看，$xz-y=0$ 定义的曲面，当 $x\to 0$ 时，曲面渐成垂直的，自然不是"平"的。▌

用同调代数的方法，我们可以重新定义平模如下。

定理9.15 M是平模的充要条件是：对任给的正合序列

$$\cdots\longleftarrow N_1\longleftarrow N_2\longleftarrow\cdots,$$

则对M作张量积以后的序列

$$\cdots\longleftarrow N_1\otimes M\longleftarrow N_2\otimes M\longleftarrow\cdots$$

仍然正合。

证明 充分性。设有下列方程式

$$\sum_{j=1}^{n} r_jx_j = 0, \quad x_j\in M, \ r_j\in R.$$

考虑下面的正合序列

$$R\overset{\sigma}{\longleftarrow}R^n\longleftarrow K\longleftarrow 0,$$

$$\sigma(t_1,\cdots,t_n) = \sum_j r_jt_j, \quad K = \ker\sigma.$$

对M作张量积，得正合序列

$$R\otimes M\overset{\bar{\sigma}}{\longleftarrow}R^n\otimes M\longleftarrow K\otimes M\longleftarrow 0,$$

即

$$M \xleftarrow{\bar{\sigma}} M^n \longleftarrow K \otimes M \longleftarrow 0,$$
$$\ker \bar{\sigma} = K \otimes M.$$

于是

$$\sum_j r_j x_j = 0 \iff \bar{\sigma}(x_1, \cdots, x_n) = 0$$
$$\iff (x_1, \cdots, x_n) \in K \otimes M$$
$$\iff (x_1, \cdots, x_n) = \sum_i k_i \otimes m_i.$$

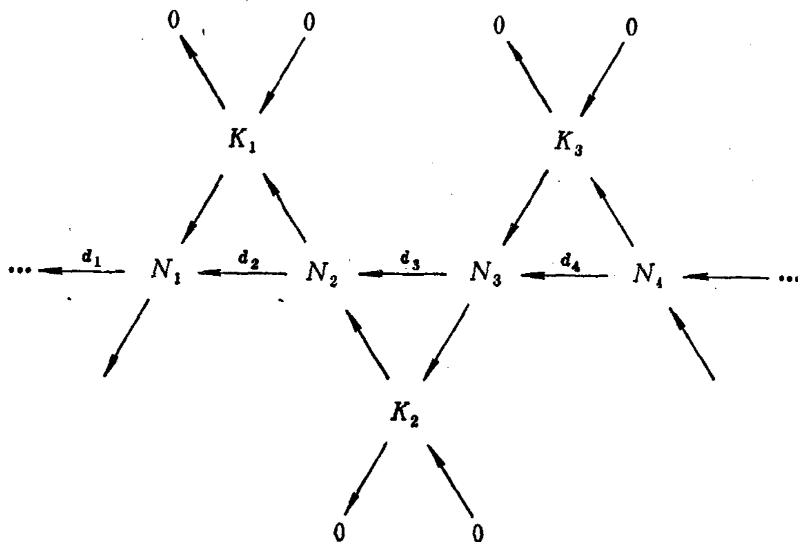
令$k_i = (s_{1i}, \cdots, s_{mi})$。则有

$$x_j = \sum_i s_{ji} m_i, \quad \sum_j r_j s_{ji} = 0.$$

必要性。任给一正合序列

$$\cdots \xleftarrow{d_1} N_1 \xleftarrow{d_2} N_2 \xleftarrow{d_3} N_3 \xleftarrow{d_4} N_4 \longleftarrow \cdots$$

都可以分解成下面的短正合序列：



其中 $K_3=\mathrm{im}d_4=\ker d_3$，$K_2=\mathrm{im}d_3=\ker d_2$，$K_1=\mathrm{im}d_2=\ker d_1$，斜线上的映射都是自然导出的. 显然，要证明

$$\cdots\longleftarrow N_1\otimes M\longleftarrow N_2\otimes M\longleftarrow N_3\otimes M\longleftarrow N_4\otimes M\longleftarrow\cdots$$

是正合的，仅须证明

$$0\longleftarrow K_{i-1}\otimes M\longleftarrow N_i\otimes M\longleftarrow K_i\otimes M\longleftarrow 0$$

都是正合的. 对张量积而言，$K_{i-1}\otimes M$ 及 $N_i\otimes M$ 两处正合性都是易证的. 我们仅证明较难的 $K_i\otimes M$ 处的正合性. 即已知

$$N\stackrel{\sigma}{\longleftarrow}K\longleftarrow 0$$

是正合的，M 是平模，求证

$$N\otimes M\stackrel{\sigma\otimes 1}{\longleftarrow}K\otimes M\longleftarrow 0$$

是正合的. 以下我们分成几步来证明：1）设 $R=N$，K 是 R 的理想；2）设 N 是自由模；3）一般情形.

1）设 $(\sigma\otimes 1)\left(\sum_j r_j\otimes x_j\right)=0$，$r_j\in K$，$x_j\in M$，即

$$\sum_j r_j\otimes x_j=0\in R\otimes M\approx M,$$

$$1\otimes\sum_j r_jx_j=0,\qquad \sum_j r_jx_j=0.$$

按照平模的定义，有 $x_j=\sum_i s_{ji}e_i$，$\sum_j r_js_{ji}=0$. 代入，得

$$\sum_j\left(r_j\otimes\sum_i s_{ji}e_i\right)=\sum_i\left(\left(\sum_j r_js_{ji}\right)\otimes e_i\right)=0\in K\otimes M.$$

2）设 $N=\oplus Rf_i$ 及 $r_j=\sum_i k_{ij}f_i$，$\sum_j r_j\otimes x_j=0\in N\otimes M$，即

$$\sum_{i,j}k_{ij}f_i\otimes x_j=\sum_i f_i\otimes\left(\sum_j k_{ij}x_j\right)=0.$$

因为 $N\otimes M=\oplus(Rf_i\otimes M)$，所以上式即

$$f_i\otimes\left(\sum_j k_{ij}x_j\right)=0,\qquad i=1,2,\cdots,$$

亦即
$$\sum_j k_{ij}f_i\otimes x_j=0.$$

以下证法与1）全同。

3）取自由模F，使$F \xrightarrow{\alpha} N \longrightarrow 0$正合。令$L=\alpha^{-1}(K)$，$P=\alpha^{-1}(0)$，则有下面左边的图：

$$
\begin{array}{ccccc}
P & = & P & & \\
\downarrow & & \downarrow & & \\
F & \longleftarrow & L & \longleftarrow & 0 \\
\downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \alpha} & & \\
N & \xleftarrow{\sigma} & K & \longleftarrow & 0 \\
\downarrow & & \downarrow & & \\
0 & & 0 & &
\end{array}
\qquad\qquad
\begin{array}{ccccc}
P\otimes M & & P\otimes M & & \\
\downarrow & & \downarrow & & \\
F\otimes M & \longleftarrow & L\otimes M & \longleftarrow & 0 \\
\downarrow & & \downarrow & & \\
N\otimes M & \longleftarrow & K\otimes M & \leftarrow\!\!-\!-\!- & 0 \\
\downarrow & & \downarrow & & \\
0 & & 0 & &
\end{array}
$$

取张量积，则得上面右边的图。显然有$F\otimes M\supset L\otimes M\supset P\otimes M$，以及

$$N\otimes M\approx F\otimes M/P\otimes M\supset L\otimes M/P\otimes M=K\otimes M. \quad \blacksquare$$

请把下面的定理与定理9.8相比。

定理9.16 对任意模M而言，下面的三个性质是等同的：

1）M是平模；

2）对所有的$n\geqslant 1$及所有的模N，$\mathrm{Tor}_n^R(M,N)=0$；

3）对所有的模N，$\mathrm{Tor}_1^R(M,N)=0$。

证明 1）$\Longrightarrow$ 2）。任取N的一个射影化解序列

$$0\longleftarrow N\longleftarrow C_0\longleftarrow C_1\longleftarrow\cdots,$$

对M作张量积。根据上定理，

$$0\longleftarrow N\otimes M\longleftarrow C_0\otimes M\longleftarrow C_1\otimes M\longleftarrow\cdots$$

也是正合的。所以$\mathrm{Tor}_n^R(M,N)=0$（$\forall n\geqslant 1$）。

2）$\Longrightarrow$ 3）。显然。

3）$\Longrightarrow$ 1）。参考定理9.15的证明，我们仅须取一个短正合序列

$$0\longleftarrow N'\longleftarrow N\longleftarrow N''\longleftarrow 0,$$

则有

$$0 \longleftarrow N' \otimes M \longleftarrow N \otimes M \longleftarrow N'' \otimes M \longleftarrow \mathrm{Tor}_1^R(M,N) = 0$$

是正合的。所以M是平模。 ▎

习　题

1. 设L,M,N是R模，证明有如下模同构：

$$\mathrm{Hom}(M \otimes N, L) \approx \mathrm{Hom}(M, \mathrm{Hom}(N,L)).$$

2. 设有R模正合序列

$$M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0,$$

N是任意R模。证明下面序列正合：

$$M' \otimes N \xrightarrow{f \otimes 1} M \otimes N \xrightarrow{g \otimes 1} M'' \otimes N \longrightarrow 0.$$

3. 设$R = \boldsymbol{Z}$，p是素数，则

$$M = \boldsymbol{Z},\ N = \boldsymbol{Z}/p\boldsymbol{Z}$$

都是R模。定义模映射正合序列：

$$0 \longrightarrow M \xrightarrow{f} M,$$

其中$f(x) = px$（对一切$x \in M$）。证明模映射序列

$$0 \longrightarrow M \otimes N \xrightarrow{f \otimes 1} M \otimes N$$

不正合。

4. 设$R = \boldsymbol{Z}$，m,n是正整数，$d = (m,n)$。又设$M = \boldsymbol{Z}/m\boldsymbol{Z}$，$N = \boldsymbol{Z}/n\boldsymbol{Z}$，$L = \boldsymbol{Z}/d\boldsymbol{Z}$均为$R$模。证明：$M \otimes N \approx L$。

5. 证明射影模都为平模。

6. 设$M_i (i \in I)$是R模。证明$M = \bigoplus_{i \in I} M_i$是平模的充要条件是：每个$M_i$都是平模。

7. 设N是R模，证明N是平模的充要条件是：从任意R模映射$f: M' \to M$是单射可推出

$$f \otimes 1: M' \otimes N \to M \otimes N$$

也是单射。

8. 设M,N是两个循环群，视其为$\boldsymbol{Z}$模，求$\mathrm{Tor}_1^{\boldsymbol{Z}}(M,N)$。

9. 设M,N是两个$\boldsymbol{Z}$模，证明$\mathrm{Tor}_1^{\boldsymbol{Z}}(M,N)$作为加法群是一个挠群(torsion group)。

§6 同调维数

我们把任意模M与射影模(或内射模)相比，自然有下面定义。

定义9.17 1) 如果

$$0 \longrightarrow C_n \longrightarrow C_{n-1} \longrightarrow \cdots \longrightarrow C_0 \longrightarrow M \longrightarrow 0$$

是M的最短的射影化解序列，则定义M的**射影维数**为n，记为$\mathrm{proj.dim}\, M = n$。如果不存在一个有限长的射影化解序列，则称$M$的射影维数为$\infty$。

2) 如果

$$0 \longrightarrow M \longrightarrow C^0 \longrightarrow C^1 \longrightarrow \cdots \longrightarrow C^n \longrightarrow 0$$

是M的最短的內射上化解序列，则定义M的**內射维数**为n，记为$\mathrm{inj.dim}\, M = n$。如果不存在一个有限长的內射上化解序列，则称M的內射维数为∞。

讨论 1) 显然，

$$\mathrm{proj.dim}\, M = 0 \Longleftrightarrow M \text{ 是射影模；}$$

$$\mathrm{inj.dim}\, M = 0 \Longleftrightarrow M \text{ 是內射模。}$$

2) 取$M = \boldsymbol{Z}/m\boldsymbol{Z}$。显然$M$不是射影$\boldsymbol{Z}$模。我们有

$$0 \longrightarrow \boldsymbol{Z} \xrightarrow{m} \boldsymbol{Z} \longrightarrow \boldsymbol{Z}/m\boldsymbol{Z} \longrightarrow 0,$$

所以$\mathrm{proj.dim}\, M = 1$。▌

我们有下面的定理：

定理9.17 设M是模，n是非负整数。则下面的条件等价：

1) $\mathrm{proj.dim}\, M \leqslant n$；

2) 对任意模N，$\mathrm{Ext}^{n+1}(M,N) = 0$；

3) 任给一个正合序列

$$0 \longrightarrow C_n \xrightarrow{d_n} C_{n-1} \xrightarrow{d_{n-1}} \cdots \xrightarrow{d_1} C_0 \xrightarrow{\varepsilon} M \longrightarrow 0.$$

如果所有的C_i $(i<n)$都是射影模，则C_n也是射影模。

证明 1) $\Longrightarrow$ 2). 取M的长度不超过n的射影化解序列

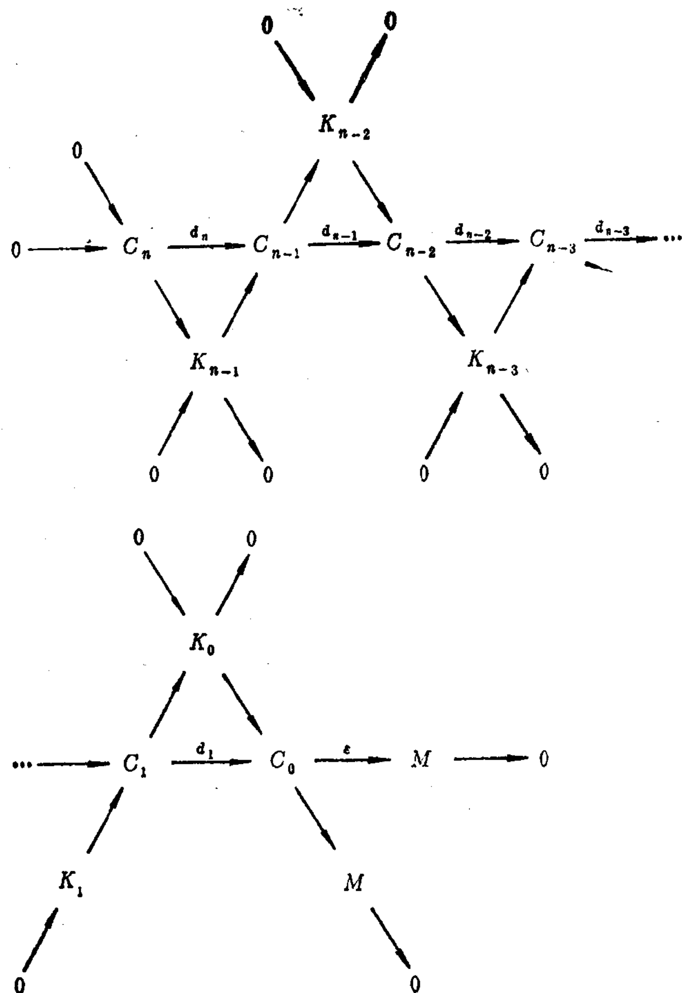
$$0\longrightarrow C_n\longrightarrow C_{n-1}\longrightarrow\cdots\longrightarrow C_0\longrightarrow M\longrightarrow 0,$$

计算$\mathrm{Ext}^{n+1}(M,N)$即可。

2) $\Longrightarrow$ 3). 把正合序列

$$0\longrightarrow C_n\longrightarrow C_{n-1}\longrightarrow\cdots\longrightarrow C_0\longrightarrow M\longrightarrow 0$$

分解成短正合序列：



此处 $K_i=\ker d_i=\operatorname{im} d_{i+1}$。应用定理9.7于短正合序列

$$0\longrightarrow K_i\longrightarrow C_i\longrightarrow K_{i-1}\longrightarrow 0,$$

以及

$$\operatorname{Ext}^j(C_i,N)=0 \quad (\forall j\geqslant 1),$$

立得

$$\operatorname{Ext}^1(K_{n-1},N)\approx\operatorname{Ext}^2(K_{n-2},N)\approx\cdots\approx\operatorname{Ext}^{n+1}(M,N)=0.$$

所以，根据定理9.8，$C_n\approx K_{n-1}$是射影模。

3)$\Longrightarrow$1)。先构造一个自由化解序列

$$C_{n-1}\xrightarrow{d_{n-1}}C_{n-2}\longrightarrow\cdots\longrightarrow C_0\xrightarrow{\varepsilon}M\longrightarrow 0.$$

令$C_n=\ker d_{n-1}$，则自然有

$$0\longrightarrow C_n\longrightarrow C_{n-1}\xrightarrow{d_{n-1}}C_{n-2}\longrightarrow\cdots\longrightarrow C_0\xrightarrow{\varepsilon}M\longrightarrow 0$$

正合。根据 3)，C_n是射影模。立得

$$\operatorname{proj.dim} M\leqslant n. \quad \blacksquare$$

例14 1) 如果环 R 是域，则任意 R 模都是向量空间，也即自由R模。此时我们恒有

$$\operatorname{proj.dim} M=0.$$

2) 如果R是主理想整环，任取R模M及一个自由R模F，使

$$F\xrightarrow{\sigma}M\longrightarrow 0$$

正合。则 $K=\ker\sigma$ 也是一个自由模。于是，立得

$$0\longrightarrow K\longrightarrow F\longrightarrow M\longrightarrow 0$$

是M的一个自由化解序列，即

$$\operatorname{proj.dim} M\leqslant 1. \quad \blacksquare$$

以上的例子表明了 proj.dim M 显示环 R 的某种性质。请见下面的定理：

定理9.18 设R是一环，n是非负整数。则下面的条件是等同的：

1) 对所有的R模M，proj.dim $M\leqslant n$；

2) 对所有的R模N，$\text{inj.dim}\, N\leqslant n$；

3) 对所有的R模M及N，$\text{Ext}_R^{n+1}(M,N)=0$。

证明 1)$\Longleftrightarrow$3)。见上面的定理9.17。

2)$\Longrightarrow$3)。应用N的长度不超过n的内射上化解序列计算$\text{Ext}_R^{n+1}(M,N)$，立得。

3)$\Longrightarrow$2)。取正合序列

$$0\longrightarrow N\longrightarrow C^0\longrightarrow C^1\longrightarrow\cdots\longrightarrow C^{n-1}\longrightarrow D\longrightarrow 0,$$

此处$C^0,C^1,\cdots,C^{n-1}$是内射模。与上面定理9.17的证明一样，我们可以得出

$$\text{Ext}^1(M,D)\approx\text{Ext}^{n+1}(M,N)=0.$$

所以D是内射模，也即上面的正合序列是N的内射上化解序列。于是$\text{inj.dim}\, N\leqslant n$。 ▌

从上面的定理，我们立即导出：对给定的环R，

$$\sup_M(\text{proj.dim}\, M)=\sup_M(\text{inj.dim}\, M).$$

定义9.18 上面的那个值(可能是∞)称为R的**整体维数**，记为$\text{gl dim}\, R$。

讨论 例14的意义是：1) 如果R是域，则有

$$\text{gl dim}\, R=0;$$

2) 如果R是主理想整环，则有

$$\text{gl dim}\, R\leqslant 1.$$

例15 我们现举一例，说明$\text{gl dim}\, R$可以是∞。令K是一域，$R=K[t^2,t^3]$。用如下的定义，可以使K成为R模：

$$f(t^2,t^3)k=f(0,0)k,\qquad k\in K.$$

我们要给出R模K的一个射影化解序列如下：

$$0\longleftarrow K\xleftarrow{\varepsilon}R\xleftarrow{d_1}R\oplus R\xleftarrow{d_2}R\oplus R\xleftarrow{d_3}R\oplus R$$

$$\xleftarrow{d_4}R\oplus R\xleftarrow{d_5}R\oplus R\longleftarrow\cdots,$$

此处我们把$R\oplus R$的元素写成直列$\begin{bmatrix}a\\b\end{bmatrix}$，而

$$d_1=\begin{bmatrix}t^3 & -t^2\end{bmatrix},\quad d_2=\begin{bmatrix}t^3 & t^2\\ t^4 & t^3\end{bmatrix},\quad d_3=\begin{bmatrix}t^3 & -t^2\\ -t^4 & t^3\end{bmatrix},$$

$$d_4=d_2,\quad d_5=d_3,\quad \cdots,$$

映射$\varepsilon, d_1, d_2, d_3$的定义即为

$$\varepsilon(f(t^2,t^3))=f(0,0),$$

$$d_1\left(\begin{bmatrix}a\\b\end{bmatrix}\right)=\begin{bmatrix}t^3 & -t^2\end{bmatrix}\left(\begin{bmatrix}a\\b\end{bmatrix}\right)=at^3-bt^2,$$

$$d_2\left(\begin{bmatrix}a\\b\end{bmatrix}\right)=\begin{bmatrix}t^3 & t^2\\ t^4 & t^3\end{bmatrix}\left(\begin{bmatrix}a\\b\end{bmatrix}\right)=\begin{bmatrix}at^3+bt^2\\ at^4+bt^3\end{bmatrix},$$

$$d_3\left(\begin{bmatrix}a\\b\end{bmatrix}\right)=\begin{bmatrix}t^3 & -t^2\\ -t^4 & t^3\end{bmatrix}\left(\begin{bmatrix}a\\b\end{bmatrix}\right)=\begin{bmatrix}at^3-bt^2\\ -at^4+bt^3\end{bmatrix}.$$

读者自行检验，上面的序列确是K的一个射影化解序列。我们现在用这个序列来计算$\operatorname{Ext}^n(K,K)$。先得到复合形

$$0\longrightarrow \operatorname{Hom}(R,K)\xrightarrow{d_1^*}\operatorname{Hom}(R\oplus R,K)\xrightarrow{d_2^*}\cdots.$$

任取$f\in\operatorname{Hom}(R,K)$及$g\in\operatorname{Hom}(R\oplus R,K)$。令

$$f(1)=k_1,\quad g\left(\begin{bmatrix}1\\0\end{bmatrix}\right)=k_2,\quad g\left(\begin{bmatrix}0\\1\end{bmatrix}\right)=k_3.$$

不难看出，任取$r\in R=K[t^2,t^3]$，有

$$f(r\cdot 1)=rf(1)=rk_1=r(0,0)k_1,$$

$$g\left(r\begin{bmatrix}1\\0\end{bmatrix}\right)=r(0,0)k_2,\quad g\left(r\begin{bmatrix}0\\1\end{bmatrix}\right)=r(0,0)k_3.$$

立得

$$(d_1^*(f))\left(\begin{bmatrix} a \\ b \end{bmatrix}\right) = f\left(d_1\left(\begin{bmatrix} a \\ b \end{bmatrix}\right)\right) = f(at^3 - bt^2)$$

$$= (at^3 - bt^2)k_1 = 0 \cdot k_1 = 0,$$

即 $$d_1^* = 0。$$

同法可知 $$d_2^* = d_3^* = \cdots = 0。$$

于是

$$\mathrm{Ext}^{n+1}(K, K) = \mathrm{Hom}(R \oplus R, K) \neq 0。$$

因此

$$\mathrm{proj.dim}\, K = \infty, \quad \mathrm{gl\,dim}\, R = \infty。 \blacksquare$$

下面的定理是"Hilbert 合冲定理"的一种形式。证法较繁，因此略去了。

定理 9.19 令K为域，$R = K[x_1, \cdots, x_n]$，其中 x_i 为变数。则有

$$\mathrm{gl\,dim}\, R = n。$$

有一个著名的"Serre猜想"。

Serre 猜想 令K为域，$R = K[x_1, \cdots, x_n]$，x_i 为变数。则任何一个射影R模M都是自由模。

在1977年，Suslin及Quillen 分别独立地证明了 Serre 猜想。与定理9.19结合，我们得出：

定理9.20 令R如定理9.19，则任意R模M都有一个长度不超过n的自由化解序列。 $\blacksquare$

习　题

1． 设环R的每个理想都是射影R模，证明对任意一个R模M，$\mathrm{proj.dim}\, M \leqslant 1$。

2． 设I是环R的理想。证明：或者R/I是射影R模，或者

$$\mathrm{proj.dim}(R/I) = \mathrm{proj.dim}(I) + 1。$$

(这里认为$+\infty=+\infty+1$。)

3. 设$0\longrightarrow M'\longrightarrow M\longrightarrow M''\longrightarrow 0$是$R$模正合序列，而$M$是射影$R$模。证明：或者三个模都是射影$R$模，或者

$$\text{proj.dim}(M'')=\text{proj.dim}(M')+1.$$

4. 设$0\longrightarrow M'\longrightarrow M\longrightarrow M''\longrightarrow 0$是$R$模正合序列。如果其中两个模射影维数有限，那么第三个模射影维数也有限。特别地，如果

$$\text{proj.dim}(M')=n,\qquad \text{proj.dim}(M'')\leqslant n,$$

那么

$$\text{proj.dim}(M)=n.$$

5. 设$0\longrightarrow M'\longrightarrow M\longrightarrow M''\longrightarrow 0$是$R$模正合序列，证明

$$\text{proj.dim}\,M''\leqslant\max\{\text{proj.dim}\,M',\ \text{proj.dim}\,M\}+1.$$

6. 设$0\longrightarrow M'\longrightarrow M\longrightarrow M''\longrightarrow 0$是$R$模正合序列，证明

$$\text{proj.dim}\,M\leqslant\max\{\text{proj.dim}\,M',\ \text{proj.dim}\,M''\}.$$

7. 证明$\text{gl}\dim R\leqslant 1$的充要条件是$R$的每个理想都是射影$R$模。

8. 试求$\text{proj.dim}(\boldsymbol{Q})$和$\text{inj.dim}(\boldsymbol{Z})$。($\boldsymbol{Q},\boldsymbol{Z}$都看作$\boldsymbol{Z}$模。)

9. 设$M_i(i\in I)$是R模，$M=\prod_{i\in I}M_i$。证明

$$\text{inj.dim}\,M=\sup\{\text{inj.dim}\,M_i\}.$$

10. 证明$\text{gl}\dim(\boldsymbol{Z})=1$。

附录　代数曲线论简介

（一）在微积分学中，我们用部分分式的方法，可以求下列积分：

(1) $$\int f(x)dx,$$

此处$f(x)$是一个一元有理函数．进一步考虑

(2) $$\int f(\sin\theta,\cos\theta)d\theta,$$

此处$f(\sin\theta,\cos\theta)$是$\sin\theta$与$\cos\theta$的有理函数．令$\sin\theta=y$，$\cos\theta=x$，那么x,y适合圆的方程式

$$x^2+y^2=1.$$

如图1，连接$(-1,0)$与$(\cos\theta,\sin\theta)$成一直线l．我们用直线l得出圆的参数方程如下：

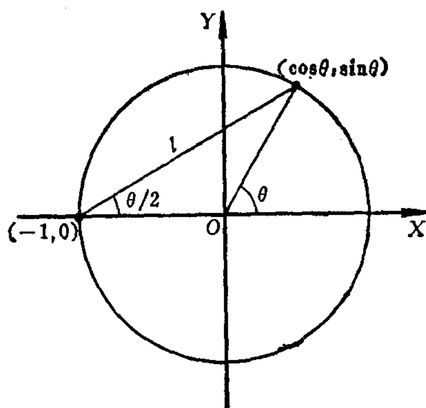


图　1

$$l:\ y=t(x+1),\qquad t=\operatorname{tg}\frac{\theta}{2}.$$

将其与圆的方程式联立求解并弃去 $x=-1$，$y=0$，得

$$x=\frac{1-t^2}{1+t^2},\qquad y=\frac{2t}{1+t^2}.$$

又有

$$-\sin\theta d\theta=dx,$$

代入(2)式，立得

$$\int f(\sin\theta,\cos\theta)d\theta=\int h(t)dt,$$

此处$h(t)$是 t 的一元有理函数。

总结上面的讨论，一般言之，我们可以讨论下列的积分：

$$\int f(x,y)dx, \tag{3}$$

此处$f(x,y)$是一个有理函数，而且x,y适合下面的代数方程

$$g(x,y)=0. \tag{4}$$

我们可以立刻把对(2)式的讨论推广到下面的情形：设(4)式有一有理参数表示式：

$$x=\alpha(t),\quad y=\beta(t),\qquad \alpha(t),\beta(t)\in C(t).$$

那么(3)式可以变换成

$$\int h(t)dt,\qquad h(t)\in C(t), \tag{5}$$

因此上式归结成(1)式，可用部分分式求积分。

由此可见，(3)式的积分问题，可以归结成(4)式所定义的“代数曲线”的性质问题。我们给出如下的定义。

定义1 由(4)式定义的代数曲线 C_1，如果有形如(5)式的有理参数表示式，则称 C_1 的亏格为 0。

（二）在数学中，有三个概念是一致的，即：

1）{无奇异点的复数射影代数曲线}；

2）{紧致黎曼曲面}；

3）{$\boldsymbol{C}$上超越次数为 1 的域 L}.

以下我们将自由地交错使用这三个概念，尤其是前两个概念。

在拓扑学中，我们知道，任取一个紧致曲面 C_1，用三角剖分(trianglization)分解 C_1，令 δ_0 为点数，δ_1为线段数，δ_2 为面数，那么，我们恒有下面的公式：

尤拉特征公式

$$\text{尤拉特征} = \chi = \delta_0 - \delta_1 + \delta_2 = 2 - 2g,$$

其中 g 是紧致曲面 C_1 的"洞数"，即亏格。

图 2 给出了亏格是 0,1,2 的图形。

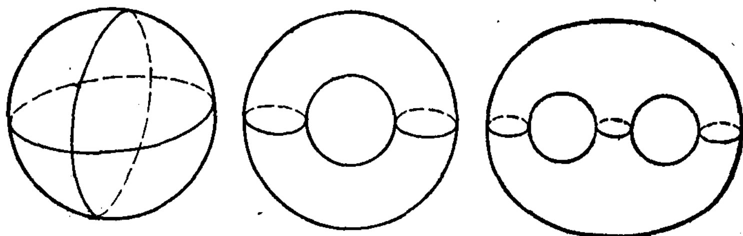


图 2

（三）以下我们要用尤拉特征公式及贝朱定理（第三章）计算一个无奇异点的平面射影代数曲线 C_1 的亏格。

设齐次式 $f(x,y,z)=0$定义了平面射影代数曲线 C_1。适当选取无穷远直线$z=0$，使$f(x,y,z)$与$f_x(x,y,z)$在 $z=0$无交点。应用贝朱定理，立得

$$\#(\{f(x,y,1)=0\}\cap\{f_x(x,y,1)=0\})=n(n-1),$$

此处 $n=\deg f(x,y,z)=C_1$ 的次数。

从代数几何的观点来看(见图 3)，$f=0$与$f'_x=0$的交点正是

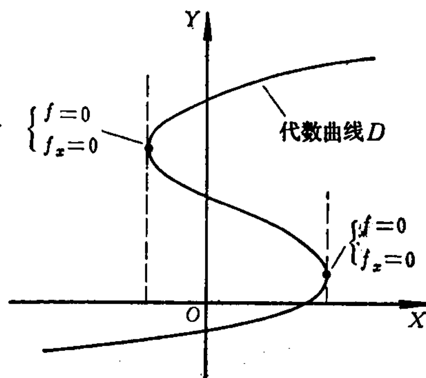


图 3

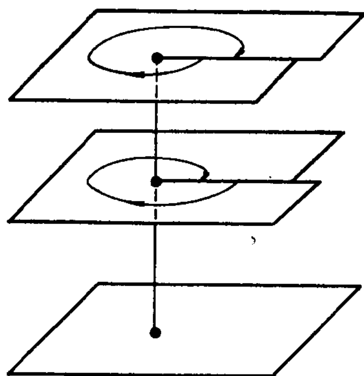


图 4

那些切线为垂直线的那些点。从黎曼曲面的观点来说，当从黎曼曲面向x轴(相当于C。加上无穷远点，即成了球面)投影时，这些点邻近的两点(或更多点)重合成一点了。因此相当于投影映射的分歧点(见图 4)。适当地选取投影方向，不妨假定，所有的垂直切线都是以二重点切于C_1。换句话说，所有的分歧点都等于二重点。

在作了上面的安排之后，我们可以如下计算C_1的亏格：在球面(x轴加上无穷远点)上选取一个三角剖分，使垂直切线在x轴上的落点，都是三角剖分的点。令球面三角剖分的点数$=\delta_0$，线

段数 $=\delta_1$，面数 $=\delta_2$。然后把这个三角剖分上升成黎曼曲面 C_1的一个三角剖分。又令它的点数 $=\Delta_0$，线段数 $=\Delta_1$，面数 $=\Delta_2$。显然，我们有下列的关系式：

$$\delta_0-\delta_1+\delta_2=2,$$

$$\Delta_0=n\delta_0-n(n-1),\qquad \Delta_1=n\delta_1,\qquad \Delta_2=n\delta_2.$$

于是算出 C_1 的亏格 g 如下

$$\Delta_0-\Delta_1+\Delta_2=2-2g,$$

$$(n\delta_0-n(n-1))-(n\delta_1)+(n\delta_2)=2-2g,$$

$$2n-n(n-1)-2=-2g,$$

即
$$g=\frac{1}{2}(n-1)(n-2).$$

不难看出，无奇异点的三次平面射影代数曲线的亏格是 1。

（四）与上面讨论类似地，我们可以得出 Hurwitz 公式如下：

$$2g_{C_1}-2=n(2g_{C_2}-2)+\sum_i(e_i-1),$$

此处自黎曼曲面 C_1 到黎曼曲面 C_2有一个 n 次代数复叠映射，g_{C_1} 是 C_1 的亏格，g_{C_2} 是 C_2 的亏格，e_i 是各点的分歧指数。

（五）我们回到积分(3)的讨论：

$$\int f(x,y)dx.$$

如果把积分号“$\int$”取消，则成了 $f(x,y)dx$，称为域 $L=\mathbf{C}(x,y)$ 的微分形式。

对于一个函数 $f\in L=\mathbf{C}(x,y)$，我们可以考虑它的零因子 $(f)_0$ (zero-divisor)及极因子 $(f)_\infty$(pole-divisor)：

$$(f)_0=\sum_i n_ip_i,\qquad (f)_\infty=\sum_j m_jq_j,$$

此处 $\sum_i n_i p_i$ 是 f 的零点的形式和，而 n_i 是零点 p_i 的重数；$\sum_j m_j q_j$ 是 f 的极点的形式和，而 m_j 是极点 q_j 的重数。与复变函数论类似，不难证明，一个有理函数的零点数等于极点数。换言之，我们有下列公式：

$$\deg(f) \equiv \deg(f)_0 - \deg(f)_\infty \equiv \sum_i n_i - \sum_j m_j = 0.$$

对于一个微分形式 fdx 及任意点 p_i，我们可以考虑 fdx/dt 在 p_i 点的零阶 n_i 或极阶 m_i，此处 t 是在 p_i 点附近的参数。如此，我们可以定义 fdx 的因子为

$$\sum_i n_i p_i - \sum_j m_j q_j,$$

以及 fdx 的次数 $\deg(fdx) = \sum_i n_i - \sum_j m_j$。任取另一微分形式 gdy，则立得

$$\frac{fdx}{gdy}$$

是一函数。因此，我们有

$$0 = \deg\left(\frac{fdx}{gdy}\right) = \deg(fdx) - \deg(gdy).$$

于是我们有下面的定义及定理。

定义2 任意微分形式 fdx 的因子 K 称为域 L 的典型因子。

定理1 域 L 的任意两个典型因子 K_1, K_2 有相同的次数。

这种典型因子的次数是多少呢？见下定理。

定理2 令超越次数为1的域 L 的亏格为 g（即与 L 相应的紧致黎曼曲面的亏格是 g），fdx 是 L 的微分形式，那么

$$\deg(fdx) = 2g - 2.$$

证明 1) 设 $g = 0$，$L = \mathbf{C}(t)$。我们仅须对 dt 证明 $\deg(dt) =$

-2。显然，在 a 点处，$t-a$是它附近的参数，以及

$$\frac{dt}{d(t-a)}=1.$$

所以dt在有限点 a 处的零阶或极阶恒为0。在无穷远点附近，$\tau=t^{-1}$是参数，以及

$$\frac{dt}{d\tau}=\frac{d\tau^{-1}}{d\tau}=-\frac{1}{\tau^2}.$$

因此 dt 在无穷远点有极阶 2。所以

$$\deg(dt)=-2=2g-2.$$

2）以下对$g>0$证明。令$L=C(x,y)\supset C(x)=F$。取 dx 为F及 L的微分形式。我们有，在对F计算时，

$$\deg(dx)=-2=2g_F-2.$$

L是F的 n 次代数重叠。对非分歧点考虑，dx对F的一个零点将上升到L为 n 个零点；同样的，dx对F的一个极点将上升到L为 n 个极点。我们再对分歧点考虑。设L的点q_i为分歧指数 e_i 的对F的 p_i 的复叠。设 q_i 点附近的参数为 t，则有

$$x=\varepsilon t^{e_i},\quad \varepsilon(q_i)\neq 0.$$

即有

$$\frac{dx}{dt}=e_i\varepsilon t^{e_i-1}+\frac{d\varepsilon}{dt}t^{e_i}.$$

于是dx在q_i点的零阶为e_i-1。综上所述，不难看出(参考Hurwitz公式)，在对 L 计算时，

$$\deg(dx)=n(2g_F-2)+\sum_i(e_i-1)=2g_L-2. \quad \blacksquare$$

（六）令D是域 L的一个因子。换句话说，

$$D=\sum_i n_ip_i-\sum_j m_jq_j,$$

以上的和是有限形式和，p_i 及 q_j 是 L 的点(即 L 的赋值)，n_i, m_j 均为非负整数。令

$$\deg D = \sum_i n_i - \sum_j m_j,$$

$$l(D) = \dim_C\{f \in L:\ (f) + D \geqslant 0\}.$$

上面的不等式$(f)+D\geqslant 0$即因子$(f)+D$中无负项的意思。我们有下列的著名定理。

Riemann-Roch定理 恒有

$$l(D) = \deg D - g + 1 + l(K - D),$$

此处K是一个典型因子。

我们不给出 Riemann-Roch 定理的证明，而是给出它的一些应用如下。

定理 3 $l((dx)) = g$。

证明 在Riemann-Roch定理中，取$D = K = (dx)$。此时

$$K - D = 0,$$

$$l(0) = \{\text{无极点的函数}\}\text{的维数} = \dim_C C = 1.$$

以定理 2 的结果代入Riemann-Roch 定理，立得

$$l((dx)) = (2g-2) - g + 1 + 1 = g. \quad \blacksquare$$

无极点的微分形式 $f dx$ 称为 L 的**正则微分形式**。

定理 4 L的所有正则微分形式构成的 C 向量空间的维数 $= g$。

证明 fdx 是正则的 $\Longleftrightarrow (fdx) = (f) + (dx) \geqslant 0$。于是自上定理立得本定理。 ▮

例 考虑下面的代数曲线C：

$$f(x, y) = y^2 - x(x-1)(x-2) = 0.$$

考虑(f, f_x, f_y)，不难看出，C在所有有限点都是非奇异的。在无穷远点来考虑，我们首先把 $f(x,y)$ 齐次化，得出

$$F(x, y, z) = y^2 z - x(x-z)(x-2z).$$

再求$z=0$时(相当于无穷远直线上)的解，即$x=0$，$z=0$，$y\neq 0$。可令$y=1$。得出

$$z - x(x-z)(x-2z) = 0.$$

此曲线在$x=0$，$z=0$点显然是非奇异的。因此我们知道此代数曲线是无奇异点的三次曲线。应用第三部分的算式，立得

$$g=\frac{1}{2}(3-1)(3-2)=1.$$

根据定理 4，我们知道有一个正则微分形式。实际上，此微分形式可以如下算出：

$$0=df=2ydy-[x(x-1)(x-2)]'dx,$$

即

$$\frac{2dy}{[x(x-1)(x-2)]'}=\frac{dx}{y}.$$

读者自证 dx/y 即是所求的正则微分形式。|

我们给出下面的定义：

定义3 设域$L\supset C$，$\operatorname{tr}\deg(L/C)=1$。那么，$L$的正则微分形式构成的 C 向量空间的维数称为L的**几何亏格**。

于是，上面的定理 4 即是说，一个无奇异点的代数曲线（或者说，一个紧致黎曼曲面）的几何亏格等于亏格。

汉英名词索引

一　画①

① 凡英文字母开始的词汇都并入一画之内。

二 画

三 画

四 画

五 画

六 画

七 画

八 画

九 画

十 画

十 一 画

十 二 画

十 三 画

十 四 画

十 六 画